

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

NETFLIX, INC. AND HULU, LLC,  
Petitioner,

v.

DIVX, LLC,  
Patent Owner.

---

IPR2020-00614  
Patent 7,295,673 B2

---

Before BART A. GERSTENBLITH, MONICA S. ULLAGADDI, and  
IFTIKHAR AHMED, *Administrative Patent Judges*.

ULLAGADDI, *Administrative Patent Judge*.

JUDGMENT

Final Written Decision

Determining All Challenged Claims Unpatentable

Dismissing In Part and Denying In Part Petitioner's Motion to Exclude

Dismissing Petitioner's Motion to Strike

Granting Patent Owner's Motion to Seal

Granting Patent Owner's Motion for Entry of Protective Order

35 U.S.C. § 318(a)

## I. INTRODUCTION

### A. Background

Netflix, Inc. and Hulu, LLC (collectively, “Petitioner”) filed a Petition to institute an *inter partes* review of claims 1–6, 9, 10, and 13–19 (“the challenged claims”) of U.S. Patent No. 7,295,673 B2 (Ex. 1001, “the ’673 patent”). Paper 3 (“Pet.”). DivX, LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). With our authorization, Petitioner thereafter filed a Preliminary Reply (Paper 9) and Patent Owner filed a Preliminary Sur-Reply (Paper 10).

We initially denied institution on September 11, 2020. Paper 11 (“DDI”). Petitioner filed a Rehearing Request (Paper 12) on October 12, 2020. We granted Petitioner’s Rehearing Request and instituted an *inter partes* review on all challenged claims on the sole ground set forth in the Petition on December 16, 2020. Paper 13 (“Institution Decision” or “Inst. Dec.”).

Patent Owner filed a Response (Paper 22, “Patent Owner’s Response” or “PO Resp.”), Petitioner filed a Reply (Paper 31, “Petitioner’s Reply” or “Pet. Reply”), and thereafter, Patent Owner filed a Sur-Reply (Paper 50, “Patent Owner’s Sur-Reply” or “PO Sur-Reply”).

An oral hearing was held on November 10, 2021, and a transcript of the hearing (Paper 67, “Tr.” or “Transcript”) has been entered into the record.

Patent Owner also filed a Motion to Seal Exhibits 2004–2006, 2010, and 2020 (Paper 26, “Mot. Seal”) accompanied by an Unopposed Motion for Entry of Protective Order (Paper 27, “Mot. Prot.”). Petitioner opposed

Patent Owner's Motion to Seal (Paper 28, "Pet. Opp. Mot. Seal") and Patent Owner replied to Petitioner's Opposition (Paper 34, "PO Reply Mot. Seal").

Petitioner timely objected to Patent Owner's evidence (Papers 23, 24, 51) and thereafter filed a Motion to Exclude Exhibits 2004–2007, 2010–2020, and 2032 (Paper 52, "Mot. Ex."). Patent Owner opposed Petitioner's Motion to Exclude (Paper 53, "PO Opp. Ex."), and Petitioner replied to Patent Owner's Opposition (Paper 58, "Pet. Reply Ex."). Petitioner also filed a Motion to Strike Exhibit 2032 and Portions of Patent Owner's Sur-Reply (Paper 55, "Mot. St."), Patent Owner opposed (Paper 61, "PO Opp. St."), and Petitioner replied to Patent Owner's Opposition (Paper 64, "Pet. Reply St.").

Petitioner objected to certain portions of Patent Owner's demonstratives. Paper 65. Patent Owner objected to certain portions of Petitioner's demonstratives. Paper 66.

#### *B. Real Party in Interest*

Petitioner identifies "Netflix, Inc. and Hulu, LLC" as the real parties in interest for this proceeding. Pet. 82. Patent Owner identifies "DivX, LLC and DivX CF Investors LLC" as the real parties in interest for this proceeding. Paper 5, 1.

#### *C. Related Proceedings*

The parties identify the following related district court proceedings: (1) *DivX, LLC v. Netflix, Inc.*, No. 2:19-cv-01602 (C.D. Cal.) and (2) *DivX, LLC v. Hulu, LLC*, No. 2:19-cv-1606 (C.D. Cal.). Pet. 82; Paper 5, 1.

#### *D. The '673 Patent*

The '673 patent concerns generating and decrypting "a protected stream of compressed video content" from "an input stream of compressed

video content containing a sequence of frames.” Ex. 1001, code (57). Specifically, a “set of encrypted frames are created by encrypting selected frames of the sequence of frames in accordance with a frame encryption function.” *Id.* Frame decryption information for decrypting the encrypted frames is included with the encrypted frames and unencrypted frames in the protected stream. *Id.* “[T]he frame decryption information includes data distinguishing the encrypted frames from the unencrypted frames of the compressed video content within the protected stream,” so that encrypted frames can be “decrypted in accordance with the frame decryption information.” *Id.*

The ’673 patent discloses an “encryption layout or frame encryption function” in which “selective placement of encrypted material consistent with an encryption layout function permits, for example, the recovered video stream to reflect a desired degree of perceived degradation or ‘scrambling.’” *Id.* at 5:32–35. Two such encryption layout approaches are “header layout” and “middle layout.” *Id.* at 5:41–43. “[H]eader layout encryption can result in a visual blackout of the associated video through placement of encrypted material within critical areas of the header portion of a given frame.” *Id.* at 5:44–47. That is, “when the applicable encryption layout or frame encryption function prescribes that the header data of a given frame is encrypted, a sufficiently large amount of video information may become unusable such that the frame is effectively ‘blacked out’ (i.e., is skipped during playback).” *Id.* at 5:36–41. “The ‘middle layout’ approach contemplates the placement of encrypted material at a location corresponding to a specified offset into the frame, which has the effect of

locating the scrambled effect within a desired area upon playback of the video containing the frame.” *Id.* at 5:49–54.

Figure 5 illustrates the header layout and middle layout examples of the encryption layout approach for a video stream formatted under the MPEG-4 standard.

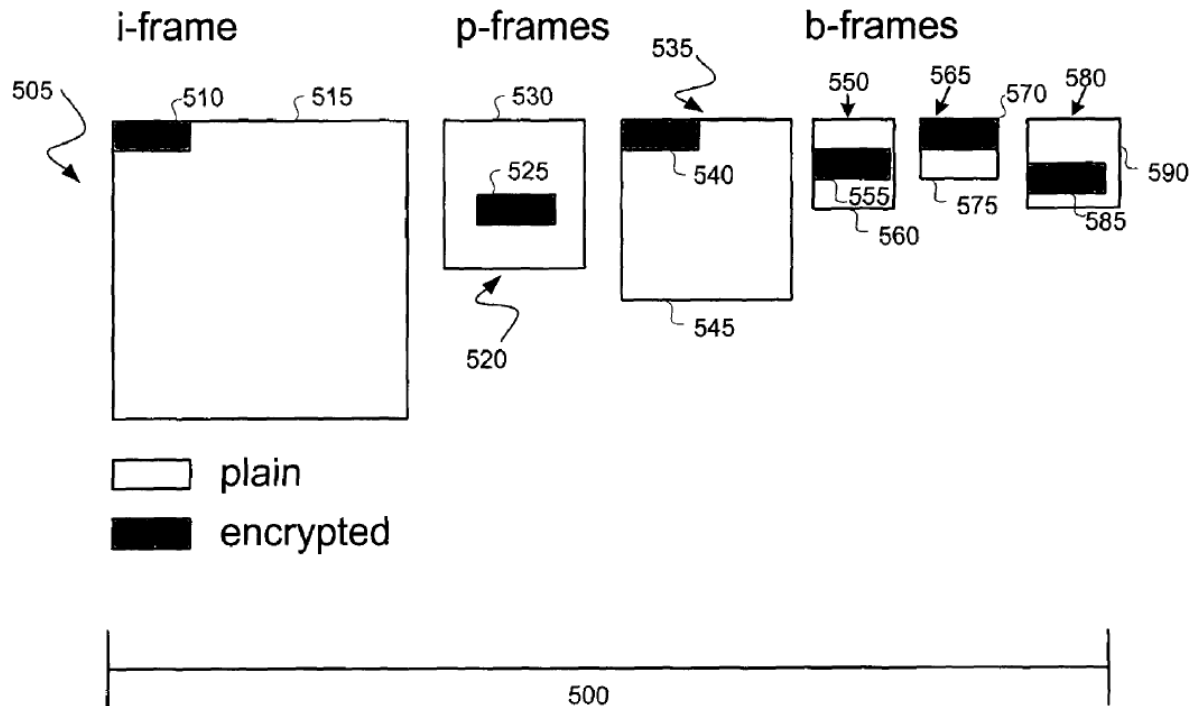


**FIG. 5**

Figure 5 “provides an overview of header layout and middle layout encryption . . . as applied to various frames formatted consistently with the MPEG-4 standard.” *Id.* at 4:61–64.

MPEG-4 video stream 500, shown in Figure 5, includes “intra frames (i-frames), predictive frames (p-frames), and bi-direction predictive frames (b-frames).” *Id.* at 5:58–60. “Encrypted portion 510 of i-frame 505 is located at the beginning of the frame, thus indicating that header layout encryption has been applied.” *Id.* at 5:62–65. Accordingly, if the video

stream were displayed without being decrypted, “the header of i-frame 505 would cause a blacked-out portion to appear in such visual display during the interval corresponding to i-frame 505.” *Id.* at 5:65–6:2. Alternatively, “[t]he encrypted portion 525 of p-frame 520 [can be] applied with an offset, thus indicating that middle layout encryption has been applied.” *Id.* at 6:5–7. In this case, if the video stream were displayed without being decrypted the p-frame would appear “as a random static-like pattern.” *Id.* at 6:7–9.

The ’673 patent further discloses applying “header and offset encryption at a predetermined frequency with respect to each frame type.” *Id.* at 8:5–7. According to the ’673 patent, “the application frequency of each type of encryption offset (i.e., header and middle offset) with respect to the various frame types can be based upon a function or series.” *Id.* at 8:11–14. For example, “a Fibonacci series could be used, resulting in a specified encryption offset being applied at frame numbers 1, 1, 2, 3, 5, 8, 13, 21” or “a non-linear function could be used so that any pattern to the offsets would be difficult to detect.” *Id.* at 8:14–18.

#### *E. Illustrative Claims*

Petitioner challenges claims 1–6, 9, 10, and 13–19 of the ’673 patent. Claims 1 and 14 are independent and are reproduced below.

1. A method for producing a protected stream of compressed video content, said method comprising:
  - receiving an input stream of compressed video content containing a sequence of frames;
  - generating a frame encryption key and storing the encryption key in a key table;
  - creating a set of encrypted frames by encrypting at least selected portions of selected frames of said sequence of frames

using the frame encryption keys in accordance with a frame encryption function;

generating frame decryption information necessary to decrypt said set of encrypted frames including an encryption key pointer identifying a decryption key to be used in the decryption of each encrypted frame; and

assembling at least said set of encrypted frames, unencrypted frames of said sequence of frames, and said frame decryption information to produce the protected stream of compressed video content;

wherein said frame decryption information is synchronized with said set of encrypted frames into a synchronized frame decryption stream.

Ex. 1001, 11:39–60.

14. A method for decrypting a protected stream of compressed video content comprising:

receiving an input stream of compressed video content containing encrypted frames and unencrypted frames;

receiving frame decryption information necessary to decrypt said encrypted frames, said frame decryption information is synchronized with said set of encrypted frames into a synchronized frame decryption stream and distinguishes said encrypted frames from said unencrypted frames;

obtaining an applicable frame decryption key from the received frame decryption information; and

decrypting selected portions of said encrypted frames using a frame decryption function in accordance with said frame decryption information, which identifies the specific portions of the frames to be decrypted and the applicable frame decryption key from the frame decryption information.

*Id.* at 12:47–64.

*F. Asserted Ground of Unpatentability*

Petitioner challenges claims 1–6, 9, 10, and 13–19 as follows. *See* Pet. 8. In support, Petitioner relies on the First and Second Declarations of

Dr. Patrick McDaniel (Exs. 1003, 1019). Petitioner also relies on the Declaration of Dr. James A. Storer (Ex. 1035).<sup>1</sup>

| Claim(s)<br>Challenged | 35 U.S.C. § | Reference(s)/Basis                                            |
|------------------------|-------------|---------------------------------------------------------------|
| 1–6, 9, 10, 13–19      | 103         | Ueno, <sup>2</sup> Fetkovich, <sup>3</sup> Demos <sup>4</sup> |

Patent Owner supports its arguments with the Declaration of Dr. Seth Nielsen (Ex. 2008).

*G. Principles of Law*

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

---

<sup>1</sup> Dr. McDaniel was not available to be deposed because of a medical condition, and, as such, we allowed Petitioner to replace him with a new expert, Dr. James A. Storer. Paper 48, 1, 7. Petitioner represented that Dr. Storer was willing to adopt the opinions set forth in Dr. McDaniel’s Second Declaration, as well as portions of Dr. McDaniel’s First Declaration that were cited in his Second Declaration. *Id.* at 2. We mitigated prejudice to Patent Owner by, *inter alia*, allowing Patent Owner to file exhibits with its Sur-Reply. *Id.* at 7.

<sup>2</sup> U.S. Patent 5,574,785, issued Nov. 12, 1996 (Ex. 1004, “Ueno”).

<sup>3</sup> U.S. Patent 7,151,832 B1, issued Dec. 19, 2006 (Ex. 1005, “Fetkovich”).

<sup>4</sup> U.S. Patent 6,957,350 B1, issued Oct. 18, 2005 (Ex. 1006, “Demos”).

As set forth in 35 U.S.C. § 103(a),

[a] patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007); accord *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007). However, Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, Petitioner must articulate a reason why a person of ordinary skill in the art would have combined the prior art references. *In re NuVasive*, 842 F.3d 1376, 1382 (Fed. Cir. 2016). The scope of the prior art includes all analogous art. *Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359 (Fed. Cir. 2020).

We analyze the asserted ground of unpatentability in accordance with these principles to determine whether Petitioner has met its burden to demonstrate by a preponderance of the evidence that the challenged claims are unpatentable.

*H. Level of Ordinary Skill in the Art*

Petitioner contends

A person of ordinary skill in the art (“POSITA”) for the ’673 patent would have had a bachelor’s degree in electrical engineering, computer science, or a similar field with at least two years of experience in streaming video security (which would include experience with video encoding and cryptography), or a person with a master’s degree in electrical engineering, computer science, or a similar field with a specialization in streaming video security.

Pet. 17 (citing Ex. 1003 ¶¶ 58–60). Dr. Nelson disagrees with Petitioner’s proposed level of ordinary skill in the art (*see* Ex. 2008 ¶¶ 34–37), but Patent Owner does not appear to cite to or rely on Dr. Nelson’s opinion as to this issue. *See generally* PO Resp. Nor does Patent Owner appear to address expressly this issue in its Patent Owner Response. *See id.*

We determine that the level of ordinary skill in the art proposed by Petitioner is consistent with the ’673 patent and the asserted prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We adopt Petitioner’s position as to that level in rendering the findings and conclusions in this Decision.

II. CLAIM CONSTRUCTION

We apply the same claim construction standard used by Article III federal courts and the United States International Trade Commission, which follow *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. 37 C.F.R. § 42.100(b) (2019). The standard includes construing each challenged claim of the ’673 patent “in accordance with the ordinary and customary meaning of such claim as understood by one of

ordinary skill in the art and the prosecution history pertaining to the patent.”  
*Id.*

*A. Frame Encryption Function and Frame Decryption Function*

Independent claim 1 recites, *inter alia*, “creating a set of encrypted frames by encrypting at least selected portions of selected frames of said sequence of frames using the frame encryption keys in accordance with a frame encryption function.” Ex. 1001, 11:46–49. Independent claim 14 recites, *inter alia*, “decrypting selected portions of said encrypted frames using a frame decryption function in accordance with said frame decryption information, which identifies the specific portions of the frames to be decrypted and the applicable frame decryption key from the frame decryption information.” *Id.* at 12:59–64.

The Petition primarily relies on its showing for “frame encryption function” as recited in claim 1 to teach or suggest the “frame decryption function” recited in claim 14. *See, e.g.*, Pet. 76. This reliance is due, in part, to the fact that the cited “references teach using symmetric algorithms,” which use the same key for encrypting and “decrypting the selected portions of encrypted frames in accordance with the frame decryption information.” *Id.* at 78 (citing Ex. 1004, 1:16–20; Ex. 1005, 6:52–56; Ex. 1006, 27:65–28:1; Pet. §§ VI.A.1, VI.A.5 (claim 4); Ex. 1003 ¶ 257). Accordingly and as we determined in our Institution Decision, “the encryption parameters are the same for encryption and decryption” in Petitioner’s challenge. Inst. Dec. 8.

For at least this reason, we resolve one of the parties’ disputes by applying our determinations for “frame encryption function,” discussed in detail below, to “frame decryption function.”

In its Petition, Petitioner does not propose to expressly construe any particular claim term and instead, contends that “[t]he challenged claims are invalid under their plain and ordinary meaning.” Pet. 18 (citing Ex. 1003 ¶¶ 108–109). In its Preliminary Response, Patent Owner contended that “frame encryption function” should be construed as “a function that determines the layout of encrypted portions of the frame.” Prelim. Resp. 23. Considering these positions and based on our review of the ’673 patent specification, we preliminarily determined that “the claim term frame encryption function requires specifying the location, by layout or offset, of a portion in a frame to which encryption is applied and the pattern of application of each layout or offset with respect to each type of frame in a set of frames” in our Decision Denying Institution. DDI 9. We maintained that preliminary determination in our Institution Decision. Inst. Dec. 7. We also determined, in our Institution Decision, “that the claimed frame decryption function is the inverse of the frame encryption function and encompasses ‘specifying the location, by layout or offset, of a portion in a frame to which decryption is applied and the pattern of application of each layout or offset with respect to each type of frame in a set of frames,’ for the reasons discussed in Section IV.B.2 [of the Institution Decision].” *Id.* at 6 (citing *id.* § IV.B.2).

Based on our review of the entire record developed during trial, we do not change our earlier determinations as to “frame encryption function” and “frame decryption function” in this Decision, except as to now further determine whether “specifying the location, by layout or offset” for each of these two claim terms includes specifying sub-frame structures, or whether this phrase is limited to specifying data units as bytes, as discussed below.

We adopt, in this Decision, the analysis of the claimed “frame encryption function” in our initial Decision Denying Institution (DDI 7–9) and do not repeat it herein. We also adopt the analysis of the claimed “frame decryption function” in our Institution Decision (Inst. Dec. 5–8) and not repeat it herein.

Patent Owner takes the position that “[t]he record supports the Board’s construction . . . .” PO Resp. 13 (citing PO Resp. 21–24; DDI 7–11). Patent Owner argues that “*Fetkovich*’s ‘encryption parameters’ specify portions of the frame to be encrypted based on the frame substructure being encrypted,” and “***not*** based on location, by layout or offset, of a portion in the frame to which encryption is applied” because “frame substructures, such as slices and macroblocks, do not . . . have a fixed ‘location’ in the frame.” *Id.* at 23. Patent Owner further argues that “frame encryption function” instead requires that “each frame is only encrypted, for example, at the *byte offset* within the frame for a specified number of *bytes* so as to ensure decryption would not exceed a certain processing cap,” which “allows processing power necessary to decrypt each frame to be bounded in advance.” *Id.* at 5 (citing Ex. 2008 ¶ 52; Ex. 1001, 1:16–20, 3:49–51, 10:30–34) (emphasis added).

Petitioner takes the position that its sole challenge “satisfies the frame encryption/decryption function by teaching, e.g., two aspects: (1) encryption algorithms and (2) a selection process that specifies portions of selected frames to encrypt/decrypt, e.g., with encryption parameters” and that its showing “meets the Board’s construction.” Pet. Reply 3 (citing Pet. 33–35; Inst. Dec. 14–16; Ex. 1019 ¶¶ 15–16). Still, Petitioner notes that it does “not agree that the claims require ‘specifying . . . the pattern of application of

each layout or offset with respect to each type of frame” because “[t]he ’673 patent uses permissive rather than restrictive language in describing this feature.” *Id.* at 3 n.1 (alteration in original) (citing Ex. 1001, 8:5–18). Petitioner argues that “while bytes are used in some embodiments, the ’673 specification uses [the] broader language of ‘units’ and makes clear that bytes are just one *non-limiting example* of the units in an encryption layout.” *Id.* at 7 (citing Ex. 1001, 6:25–38 (“In an exemplary embodiment . . . twelve data *units* (e.g., *bytes*) would be encrypted at the location consistent with the applicable encryption layout format” (emphasis added)); Ex. 1019 ¶ 23); *see also id.* at 9 (citing Ex. 1001, 6:31–35, 8:1–4, 8:21–24) (Petitioner arguing that “[t]he ’673 patent states that the location of encrypted portions may be specified based on ‘units’”). In the same vein, Petitioner persuasively argues that, “[i]gnoring the broader disclosures in the specification, PO [Patent Owner] asks the Board to limit ‘frame encryption/decryption function’ to specific examples. This is improper, and the Federal Circuit has repeatedly warned against it.” *Id.* (citing *Phillips*, 415 F.3d at 1323; *Nazomi Commc’ns, Inc. v. ARM Holdings, PLC*, 403 F.3d 1364, 1369 (Fed. Cir. 2005)).

Petitioner further argues that during prosecution, the Examiner cited portions of U.S. Patent No. 5,805,700 (Ex. 1010, “Nardone”) that “do not explicitly specify location/size using bytes,” and that “Applicant appears to have conceded that Nardone teaches the frame encryption function by amending claim 1 to add other limitations including, e.g., a key table.” *Id.* at 11 (citing Ex. 1002, 72–73, 92; Ex. 1010, 4:14–5:9). Petitioner asserts that “Applicant never mentioned bytes or sub-frame structures” during prosecution. *Id.*

In response to Patent Owner’s argument that “*slices* and macroblocks do not ‘have a *fixed* “location” in the frame,” Petitioner argues “the ’673 patent does not require the location of the encrypted portion to be the same for each frame—in some embodiments the location of the encrypted portion for each frame varies.” *Id.* at 10 (citing PO Resp. 23; Ex. 1001, Fig. 5, 6:3–24). Petitioner also argues that Patent Owner

contradicts its own district court allegations, which rely on encrypting portions of *slices* within a frame (which, according to [Patent Owner], change location). For the frame encryption function, [Patent Owner] accuses H.265 encryption of selected [Network Abstraction Layer (“NAL”)] units (*slices*), including parameters that specify portions of NAL units within a frame to encrypt.

*Id.* (citing Ex. 1024, 17–21 (“For example, within the first sample, subsample 8 is an IDR slice (as shown below), a NAL unit containing video information. This subsample contains 80 encrypted bytes and 11 unencrypted bytes.”)); *but see* PO Sur-Reply 13–14 (citing Ex. 1024, 19–20) (Patent Owner arguing that Petitioner is “wrong” for characterizing its District Court infringement contentions as pointing to frame sub-structures to teach the claimed “frame encryption function” and instead argues that Patent Owner “alleged that infringing devices identify both the encryption location and size based on the number of bytes, referred to as “NumClearBytes” and “NumEncryptedBytes”). Petitioner argues that “[a]s PO admits, a NAL unit is a slice” and that “PO alleged the frame encryption function is satisfied by specifying the location of encrypted portions of a frame *based on slices*,” which are “(NAL units) [that] are variable in size and not ‘fixed’ bytes that PO now contends are necessary.” Pet. Reply 10 (citing Ex. 1024, 22 (“The IDR *slice* and TRAIL\_R *slices* discussed above

are VCL *NAL units* and carry frame information.” (emphasis added)); Ex. 1025, 23, 29, 52, 82; Ex. 1029, 178:14–180:17, 187:25–189:22, 193:10–194:8).

We determine that Petitioner’s position—that the layout or offset specified by the frame encryption function *can* be specified in terms of “sub-frame structures,” such as slices or macroblocks—is the better one.

The ’673 patent discloses that “specification of an encryption quantity of 12 (i.e.,  $n=12$ ) means that in every frame subject to encryption, twelve *data units* (e.g., *bytes*) would be encrypted at the location consistent with the applicable encryption layout format.” Ex. 1001, 6:31–35 (emphasis added). The ’673 patent further discloses that “[t]he offset may range from one up to a maximum value equivalent to the frame size less the number of bytes to encrypt.” *Id.* at 7:59–61; *see also id.* at 9:35–39 (“the frame decryption information identifies, with respect to each frame of encrypted video stream 950, the frame number, the status of encryption (on encryption or off), the offset length, the number of bytes encrypted, and a reference to the applicable encryption key”), 9:50–54 (“With an offset of zero, encryption begins immediately after video object plane start code 952 and continues for  $n$  bytes. The byte encryption quantity,  $n$ , is also stored within the portion of the frame decryption information 995 corresponding to the first frame 954.”), 7:59–61, 8:24–26.

We agree with Petitioner that Patent Owner “seeks to limit the Board’s construction to specific examples in the ’673 specification.” Pet. Reply 12. “We depart from the plain and ordinary meaning of claim terms based on the specification in only two instances: lexicography and disavowal” in which “[d]isavowal requires that ‘the specification [or

prosecution history] make[] clear that the invention does not include a particular feature,’ or is clearly limited to a particular form of the invention.” *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371–72 (Fed. Cir. 2014) (citing *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)). None of the cited portions of the ’673 patent nor the cited portions of the prosecution history make clear that “frame encryption function” is limited to specifying layout or offset only in bytes, or any other specific type of data unit. *See Thorner*, 669 F.3d at 1366–67 (holding that it is “not enough that the only embodiments, or all of the embodiments, contain a particular limitation,” that limitations are not read “from the specification into claims” and that, “[t]o constitute disclaimer, there must be a clear and unmistakable disclaimer”).

In each relevant disclosure in the ’673 patent, “bytes” are an exemplary data unit of encryption or decryption, not a required unit, and in one cited portion, bytes are *expressly disclosed* as being an exemplary form of data unit. *See* Ex. 1001, 6:31–35. We are persuaded by Petitioner that, “[e]ven if those examples had benefits, it would still be improper to limit the claims to those examples because none of the purported benefits constitute ‘clear and unmistakable’ disavowal of embodiments lacking the benefits.” *Pet. Reply 12* (citing *i4i Ltd. P’ship v. Microsoft Corp.*, 598 F.3d 831, 844 (Fed. Cir. 2010), *aff’d*, 564 U.S. 91 (2011)).

*B. Synchronized Frame Decryption Stream*

Claim 1 recites

generating frame decryption information necessary to decrypt said set of encrypted frames including an encryption key pointer identifying a decryption key to be used in the decryption of each encrypted frame; and assembling at least said set of encrypted

frames, unencrypted frames of said sequence of frames, and said frame decryption information to produce the protected stream of compressed video content; wherein said frame decryption information is synchronized with said set of encrypted frames into a *synchronized frame decryption stream*.

Ex. 1001, 11:50–53 (emphasis added).

Claim 14 recites “receiving frame decryption information necessary to decrypt said encrypted frames, said frame decryption information is synchronized with said set of encrypted frames into a *synchronized frame decryption stream* and distinguishes said encrypted frames from said unencrypted frames.” *Id.* at 12:51–56.

Neither party proposes an express definition for this term.

According to Patent Owner, the Petition premises its sole ground on the allegation that “[a] POSITA’ would *modify* or *combine* its references in order to disclose ‘embedding the decryption information *for each frame* of the protected data stream before the data of the corresponding video frame’” [and] does not challenge the fact that a “synchronized . . . stream” should be construed to require decryption information for every encrypted frame. PO Resp. 36 (alteration in original) (citing Pet. 47, 50 (“A POSITA would have been motivated to apply Ueno’s teaching by including frame decryption information with each frame . . . .”)). Patent Owner contends “that merely sending frame decryption ‘information’ is not sufficient to meet these limitations: rather, the information must be sent in a ‘stream.’” *Id.* (citing Ex. 1002, 142 (Notice of Allowance, Examiner’s Amendment)); *see also* PO Sur-Reply 16 (Patent Owner arguing that “‘synchronized frame decryption stream’ requires . . . a 1:1 synchronized correspondence between the decryption information and an encrypted frame”).

Patent Owner further contends that sending encryption parameters only when the parameters are updated does not teach or suggest the claimed “synchronized frame decryption stream.” PO Resp. 37–38. According to Patent Owner, the ’673 patent “identifies the frame number to which the encryption information corresponds so that the encryption information is linked and synchronized with its corresponding frame.” *Id.* at 57. The deficiency in Petitioner’s challenge, Patent Owner contends, is that it “seems to assume that interleaving the encryption key in between frames would result in a synchronized frame decryption stream,” but that “in a lossy transmission system, interleaving the keys between frames does not synchronize them with frames.” *Id.* at 56 (citing Pet. 7 (“Decryption information was commonly interleaved with frames, and in that sense was synchronized with the frames .....”))).

Petitioner contends that Patent Owner “argues frame decryption data must be sent with each frame and include frame numbers,” but “never explains why this would be necessary, other than suggesting the claim should be limited to the embodiment of FIG. 9.” Pet. Reply 15 (citing PO Resp. 33, 45, 57–58). Petitioner presents two alternative positions on how the combination of Ueno, Fetkovich, and Demos teaches or suggests the claimed “synchronized frame decryption stream.” According to its first position, Petitioner contends that “the combination begins with Ueno’s key table and its teaching that, ‘in some cases, the cipher key number is . . . *transmitted with each of [the] frames.*’” *Id.* at 16 (first alteration in original) (citing Ex. 1004, 2:5–9; Pet. 50–51). Petitioner explains that “Fetkovich’s encryption parameters are included with Ueno’s key number, which is sent with each frame.” *Id.* at 16–17 (citing Pet. 20; Ex. 1003 ¶ 115). Thus,

according to this first alternative position, Petitioner implicitly construes “synchronized frame decryption stream” as requiring the sending of “frame decryption information” with *each* frame, presumably because the “frame decryption information” includes “an encryption key pointer identifying a decryption key to be used in the decryption of *each* encrypted frame,” as recited in claim 1. Petitioner’s first alternative position corresponds to Patent Owner’s position, which requires “a 1:1 synchronized correspondence between decryption information and an encrypted frame.” *See* PO Sur-Reply 16.

In its second alternative position implicitly construing “synchronized frame decryption stream,” Petitioner contends that “the claims would allow one chunk of decryption data to correspond to several frames.” *Pet. Reply* 24–25. Petitioner explains that “[w]hen keys/parameters are only sent when changed, that ‘decryption information is used to decrypt each frame’ until ‘the last frame before new encryption parameters are received.’” *Id.* (citing *Ex. 1003* ¶ 175; *Pet. 42*). According to Petitioner, “each frame has corresponding decryption data” and “[t]he keys/parameters are interleaved with corresponding video frames into a stream and *provide* decryption information for each frame.” *Id.* (citing *Ex. 2009*, 95:5–15; *Ex. 1003* ¶ 184; *Ex. 1005*, 7:35–50, 7:55–67) (emphasis added).

The ’673 patent depicts, in Figure 9, an “exemplary embodiment” in which “the frame decryption information 995 identifies, with respect to each frame of encrypted video stream 950, the frame number, the status of encryption (on or off), the offset length, the number of bytes encrypted, and a reference to the applicable encryption key.” *Ex. 1001*, 9:35–39, 9:27–30. The ’673 patent further discloses that “[i]n the exemplary embodiment[,] the

decryption information 995 may be incorporated within or otherwise transmitted in conjunction with the encrypted video stream 950.” *Id.* at 9:27–30. Nowhere does the ’673 patent indicate that the frame decryption information *must* be sent with *each* corresponding frame according to a 1:1 correspondence. Even if every embodiment were to disclose or depict a synchronized frame decryption stream with a 1:1 correspondence between frame decryption information and corresponding frame, the Federal Circuit has “repeatedly held that it is ‘not enough that the only embodiments, or all of the embodiments, contain a particular limitation’ to limit claims beyond their plain meaning.” *Unwired Planet, LLC v. Apple Inc.*, 829 F.3d 1353, 1359 (Fed. Cir. 2016) (citing *Thorner*, 669 F.3d at 1366; *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014)).

The specification of the ’673 patent does not support limiting “synchronized frame decryption stream” to frame decryption information sent with *each* frame in a 1:1 correspondence. Instead, we determine that Petitioner’s position that “synchronized frame decryption stream” encompasses providing “one chunk of decryption data [] correspond[ing] to several frames” is consistent with the disclosures of the ’673 patent. Pet. Reply 25.

We further note that claim 1’s encrypted frames, unencrypted frames, *and* frame decryption information are assembled into a protected stream of compressed video content. By virtue of its inclusion in the “protected stream of . . . content,” the frame decryption information is already in a stream format and synchronized with the claimed “set of encrypted frames.” Thus, whatever is cited to teach the claimed “assembling” limitation and in particular, “protected stream of compressed video content,” is also sufficient

to teach the “synchronized frame decryption stream.” The “synchronized frame decryption stream” does not require any particular sort of correlation with the frames, unencrypted and encrypted, for the frame decryption information to be considered “synchronized” with the same or to be considered to have a “stream” format. Interleaving frame decryption information, as disclosed and depicted in the ’673 patent, to include frame decryption information between encrypted and unencrypted frames is sufficient. *See* Pet. Reply 14 (citing Pet. 50; Ex. 1011 (DivX Amended Complaint Against Netflix) ¶ 276).<sup>5</sup>

As such, Patent Owner’s interleaving arguments, which make reference to the type of transmission system (i.e., lossy or lossless) as a qualifier for including frame decryption information in a 1:1 correspondence with the encrypted frames, are unavailing. *See* PO Resp. 55–57.

For the foregoing reasons, we determine that “synchronized frame decryption stream” encompasses frame decryption information that is provided when there is a key update in an interleaved fashion with said set of encrypted frames. The claim term does not require sending frame decryption information with *each* corresponding frame in a 1:1 correspondence, contrary to Patent Owner’s arguments.

---

<sup>5</sup> Our finding is consistent with Patent Owner’s position taken in district court in which it argued that “Netflix’s ‘frame decryption information is synchronized with said set of encrypted frames into a synchronized frame decryption stream’ when Netflix synchronizes the frame decryption information by interleaving the PIFF Sample Encryption Boxes (uuid) and media data, or “mdat,” boxes throughout the MP4 file.”). Ex. 1011 ¶ 276.

### III. ANALYSIS

#### A. *Challenge to Claims 1–6, 9, 10, and 13–19*

Petitioner asserts that claims 1–6, 9, 10, and 13–19 would have been obvious over Ueno, Fetkovich, and Demos. *See* Pet. 18–82. For the reasons that follow, we are persuaded that Petitioner establishes unpatentability of the challenged claims over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

##### 1. *Ueno (Ex. 1004)*

Ueno concerns “[a]n enciphered communication system . . . which has a plurality of cipher keys selectively used for enciphering data, wherein even when a cipher key number used at a transmitting side is not correctly transmitted to a receiving side, the receiving side can change the cipher key to a correct one.” Ex. 1004, code (57). The transmitter and receiver “are each provided with a plurality of cipher keys, a cipher key number is allotted to each cipher key, and a collation table consisting of the cipher keys and the cipher key numbers corresponding thereto is stored in each of the cipher key tables.” *Id.* at 5:15–20. To change a cipher key, Ueno discloses setting a “cipher key number N(ks) so that a corresponding one of the pre-stored cipher keys ks may be selected.” *Id.* at 5:20–23. “[T]he cipher key number N(ks) is notified to the receiving side” via a multiplexing section of the transmitter, which “multiplex[es] the enciphered data and the cipher key number N(ks).” *Id.* at 5:27–29, 4:55–57.

##### 2. *Fetkovich (Ex. 1005)*

Fetkovich concerns “[d]ynamic varying of encrypting of a stream of data at an encryption unit based on data content.” Ex. 1005, code (57). The variation in encryption “can be responsive to passage of a predefined

number of units of physical data or passage of a predefined number of conceptual units of data, [and] is accomplished by changing at least one encryption parameter over different portions of the data.” *Id.* For example, in “an MPEG video data stream, this might mean that after a certain number of macroblocks, slices, fields, frames, pictures, groups of pictures (GOPs), or sequences have been sent and received, an encryption parameter (such as an encryption key) is automatically updated.” *Id.* at 4:13–18.

3. *Demos (Ex. 1006)*

Demos concerns “[a] method and apparatus for image compression using temporal and resolution layering of compressed image frames, and which provides encryption and watermarking capabilities.” Ex. 1006, code (57). Demos discloses “[e]ncryption preferably operates in a fashion as to scramble, or at least visibly impair, as many frames as possible from the smallest possible units of encryption.” *Id.* at 22:29–31. For MPEG systems, which “utilize a hierarchy of units of information which must be processed in cascade in order to decode a range of frames (a ‘Group of Pictures,’ or GOP),” “not every unit need b[e] encrypted or confounded by the encryption of a higher-level unit.” *Id.* at 22:32–36, 22:40–41. “Thus, in selecting units to encrypt, it is useful to note how encryption of particular units can confound the usability of other related units.” *Id.* at 23:23–25.

4. *Claim 1*

a) *Element-by-Element Analysis of Claim 1*

*[1a] A method for producing a protected stream of compressed video content, said method comprising:*

Although Petitioner contends that the proposed combination “teaches or suggests a method for producing a protected stream of compressed video

content (e.g., the partially-encrypted stream described in the analysis for the rest of claim 1),” Petitioner shows how each of the references, individually, teaches the preamble of claim 1. Pet. 29 (citing Ex. 1003 ¶¶ 144–145). For example, Petitioner contends “Fetkovich teaches producing a protected stream of compressed digital video content.” *Id.* (citing Ex. 1005, 1:16–19; 6:49–65, 7:8–27, Fig. 2). Petitioner presents similar arguments for Demos and Ueno. *Id.* (citing Ex. 1006, 21:20–22, Fig. 13 (arguing “Demos further teaches this limitation”); Ex. 1004, code (57), 1:33–43, 2:50–67, 5:15–32, 6:54–59 (arguing “Ueno teaches a method for encrypting content and creating a stream of protected data frames”))).

We are persuaded that the cited portions show how Ueno, Fetkovich, and Demos each individually teach the subject matter of the preamble of independent claim 1. We need not determine whether the preamble of claim 1 is limiting because Petitioner shows sufficiently that the subject matter is taught by the references.

*[1b] receiving an input stream of compressed video  
content containing a sequence of frames;*

Although Petitioner contends that the proposed combination discloses “receiving an input stream of compressed video content (such as MPEG) containing a sequence of frames, in order to encrypt it,” Petitioner points out where, individually, Fetkovich and Demos each teach limitation [1b]. Pet. 29–30 (citing Ex. 1005, 3:4–14, 6:49–57, Fig. 1; Ex. 1006, 21:10–13, 21:20–22, 22:29–39, 23:30–24:19; Ex. 1003 ¶¶ 146–149). Petitioner contends that “[t]he stream of compressed video content contains a sequence of frames; as was widely known, MPEG video contains a sequence of

frames/pictures.” *Id.* at 30 (citing Ex. 1005, 4:37–44; Ex. 1006, 22:63–23:7; Ex. 1003 ¶¶ 148–149).

We are persuaded that the cited portions show how Fetkovich and Demos each individually teach limitation [1b].

*[1c] generating a frame encryption key and storing  
the encryption key in a key table;*

Petitioner contends that individually “[t]he references teach generating a frame encryption key. . . .” Pet. 30–31 (citing Ex. 1005, 6:49–52 (teaching “a dynamic key generator”), Fig. 1; Ex. 1006, 28:1–9 (“Next, one or more keys are generated (STEP 1304) .....”), Fig. 13; Ex. 1003 ¶ 150). Petitioner further contends that “Ueno teaches storing encryption keys in a key table.” *Id.* at 31 (citing Ex. 1004, 1:53–57 (“Thus, the transmitter 1 and the receiver 2 have identical cipher key tables 12 and 23, respectively, each having a plurality of cipher keys..... ”), Fig. 16).

We are persuaded by Petitioner’s contentions and the cited portions of Ueno, Demos, and Fetkovich that the combination teaches limitation [1c].

We discuss Petitioner’s motivation to combine Ueno, Fetkovich, and Demos in Sections III.A.4.b and III.A.4.c.

*[1d] creating a set of encrypted frames by encrypting  
at least selected portions of selected frames of said  
sequence of frames using the frame encryption keys  
in accordance with a frame encryption function;*

According to a first theory, Petitioner relies on Fetkovich and Demos to teach this limitation. *See* Pet. 33–35. “Fetkovich teaches encryption parameters to select which slices or macroblocks in a frame are encrypted, including ‘encryption granularity, an encryption density scale, an encryption density, an encryption delay.’” *Id.* at 33 (citing Ex. 1005, 3:4–14, 5:38–56,

6:24–40; Ex. 1003 ¶¶ 155–156). Petitioner relies on Demos to teach selecting which frames to encrypt. *Id.* (citing Pet. § VI.A.1; Ex. 1003 ¶ 154; Ex. 1005, 4:37–44; Ex. 1006, 22:29–58, 23:8–24:18, Fig. 11). According to Petitioner, the combination therefore “teaches creating a set of encrypted frames by encrypting at least selected portions of selected frames, which are satisfied [in] at least three independent ways: (1) I and P frames; (2) every other minute of video frames; or alternatively, (3) frames of particularly important plot or action scenes.” *Id.* at 33–34 (citing Pet. § VI.A.1; Ex. 1006, 22:29–44, Fig. 11). Each of the three ways “creates a set of encrypted frames (the frames selected for partial encryption) and a set of unencrypted frames (the other frames that are left unencrypted).” *Id.* at 34 (citing Ex. 1003 ¶ 157).

Petitioner further contends that “Fetkovich teaches creating a set of encrypted frames using the frame encryption keys in accordance with a *frame encryption function*” and that “*encryption algorithms and encryption parameters together control the encryption process, including the portions of the video stream to encrypt.*” *Id.* at 35 (emphasis added) (citing Ex. 1005, 3:4–14, 5:9–6:40, 6:49–65 (“Sender 12 includes an encryption unit 20 which (in this example) receives as inputs an encryption key from a dynamic key generator 22, and the unencrypted, but encoded MPEG data stream. Any conventional encryption technique can be employed within encryption unit 20.....”), Fig. 1; Ex. 1003 ¶¶ 158–159, 161).

Petitioner presents a second, alternative theory in which it relies on Demos individually to teach this limitation. According to Petitioner,

Demos by itself teaches or suggests the creation of a set of encrypted frames by encrypting at least selected portions (e.g., DC coefficients or AC coefficients) of selected frames (e.g., I-

frames, or I and P-frames) of said sequence of frames using the frame encryption keys in accordance with a frame encryption function (e.g., using DES, Triple DES, or Blowfish *to encrypt selected portions of selected frames*).

Pet. 35 (citing Ex. 1003 ¶¶ 162–169) (emphasis added). Petitioner also contends “Demos further teaches ‘an entire frame need not be encrypted . . . Sub-units of frames may be encrypted and still have a confounding affect [sic], while reducing encryption and decryption processing time.’” *Id.* at 37 (alterations in original) (citing Ex. 1006, 23:37–24:18, Table 8).

Petitioner contends that “[a] POSITA would have been motivated to select I-frames, or I and P-frames, for partial encryption because Demos teaches that they have ‘high influence’ and are thus ‘better for encryption.’” *Id.* at 36 (citing Ex. 1006, Fig. 11, 22:53–58; Pet. § VI.A.1; Ex. 1003 ¶ 164). Petitioner further contends that “I-frames have the highest influence, but when computational power is available, selecting both I and P-frames provides additional security for different types of content, with a favorable efficiency balance.” *Id.* (citing Ex. 1006, Fig. 11; Ex. 1003 ¶ 163).

We are persuaded by Petitioner’s contentions, Dr. McDaniel’s testimony, and the cited portions of Demos and Fetkovich that the combination teaches limitation [1d], under either of Petitioner’s alternative positions.

*[1e] generating frame decryption information  
necessary to decrypt said set of encrypted frames  
including an encryption key pointer identifying a  
decryption key to be used in the decryption of each  
encrypted frame; and*

Petitioner contends that “Ueno teaches storing encryption keys in key tables where ‘a cipher key number is allotted to each cipher key[.]’” Pet. 40

(alteration in original) (citing Ex. 1004, 5:14–20, 1:53–57, 6:54–59; Pet. § VI.A.2[1c]). Petitioner further contends that “Ueno further teaches ‘a cipher key number sending section’ that generates key numbers (e.g., ‘N(ks)’), *which are periodically transmitted to the receiver*, multiplexed into the data stream, to facilitate decryption of the data stream by identifying the key to be used for decrypting each *portion* of the data stream.” *Id.* (emphasis added) (citing Ex. 1004, 1:32–42, Fig. 16). More particularly, Petitioner contends Ueno teaches: (1) *sending the key number periodically*; (2) *with each frame*; or (3) *when the key is changed*. *Id.* (citing Ex. 1004, 2:5–9, 6:35–39, 7:28–32). Petitioner explains that “[w]hen *the key number is included periodically*, the decryption information is used to decrypt each frame starting from the frame for which the key number was sent and ending with the last frame before a new key number is received.” *Id.* at 42 (emphasis added) (citing Ex. 1003 ¶ 174). Petitioner further explains “Ueno’s multiplexed key numbers are encryption key pointers that identify a decryption key to be used in the decryption of each encrypted frame; each key number identifies a decryption key.” *Id.* at 41 (citing Ex. 1004, 1:53–57 (“[O]nly the cipher key number corresponding to the cipher key which is used to encipher the transmit data is transmitted to the receiver 2.”), 5:14–20; Ex. 1003 ¶ 172; Pet. § VI.A.1).

According to Petitioner, “[i]n this way, the sender of the data stream communicates to the receiver a key number corresponding to each frame, for use as a pointer identifying the decryption key in decrypting the frame.” *Id.* at 41 (citing Ex. 1004, 1:43–60 (“The receiving side decodes the received data to acquire the cipher key number, and obtains the same cipher key as

used at the transmitting side from the cipher key number to decipher the data.”); Ex. 1004, 4:60–5:3, 5:32–44, 6:60–67).

Petitioner contends that “Fetkovich teaches generating encryption parameters that control the encryption process—including partial encryption and the timing of how frequently keys are updated—which are necessary to decrypt frames.” *Id.* at 42 (citing Ex. 1005, 7:8–27, 6:66–7:7; Ex. 1003 ¶ 175). Petitioner explains that “[a] POSITA would have understood Ueno’s key numbers and Fetkovich’s encryption parameters to be frame decryption information because they are used to control the decryption process and are necessary for decrypting video frames.” *Id.* at 42–43 (citing Pet. §§ VI.A.2[1d], VI.A.1; Ex. 1001, Fig. 9, 9:23–39).

Petitioner further explains that “[w]ith symmetric encryption, a POSITA would have understood the prior art teachings of key numbers and encryption parameters to be both frame encryption information and frame decryption information.” *Id.* at 43 (citing Ex. 1003 ¶ 177).

We are persuaded by Petitioner’s contentions, Dr. McDaniel’s testimony, and the cited portions of Ueno and Fetkovich that the combination teaches limitation [1e]. We find persuasive Ueno’s teaching of sending a key number periodically and its teaching of sending the key number when the key is changed. *See* Pet. 40 (citing Ex. 1004, 2:5–9, 6:35–39, 7:28–32). We make this determination regarding only Petitioner’s second alternative position (sending one chunk of decryption data to correspond to several frames), and not its first alternative position (arguing a 1:1 correspondence between frame decryption information and frames). *Supra* § II.B; Pet. Reply 24–25.

*[1f] assembling at least said set of encrypted frames, unencrypted frames of said sequence of frames, and said frame decryption information to produce the protected stream of compressed video content;*

Petitioner contends that “Ueno teaches assembling the sequence of frames and key numbers by multiplexing them into a single protected stream.” Pet. 43 (citing Ex. 1004, 1:67–2:9 (“[T]he data transmitted onto the transmission line 3 from the transmitter 1 consists of input data D enciphered by the data enciphering section 11, the cipher key number N(ks) output from the cipher key number sending section 14 and multiplexed at the multiplexing section 15, and frame synchronizing signals F .....”), Fig. 17; Ex. 1003 ¶ 179).

Petitioner further contends that “Fetkovich further teaches assembling the sequence of frames—including encrypted and unencrypted frames—and the frame decryption information by multiplexing them into a single stream.” *Id.* at 45 (citing Ex. 1005, 6:49–65 (“[T]he encrypted MPEG stream is fed to a data multiplexer 24 which multiplexes into the stream . . . the encryption parameters employed by the encryption unit.”), 7:8–27, 5:34–56, 6:6–7, Fig. 1; Ex. 1003 ¶ 180).

Petitioner contends that “[a] POSITA would have recognized Ueno’s key number and Fetkovich’s encryption parameters to be frame decryption information.” *Id.* at 46 (citing Pet. §§ VI.A.1, VI.A.2[1e]; Ex. 1003 ¶ 181).

We are persuaded by Petitioner’s contentions, Dr. McDaniel’s testimony, and the cited portions of Ueno and Fetkovich that the combination of Ueno, Fetkovich, and Demos teaches limitation [1f].

*[1g] wherein said frame decryption information is synchronized with said set of encrypted frames into a synchronized frame decryption stream.*

Petitioner contends that “[t]he combination teaches or suggests multiplexing periodic frame decryption information—including key numbers and partial encryption parameters—into the video stream, by embedding the decryption information for each frame of the protected data stream before the data of the corresponding video frame.” Pet. 46–47 (citing Pet. §§ VI.A.2[1e–1f]; Ex. 1003 ¶ 182).

Specifically, Petitioner contends that “Ueno [] teaches that frame synchronization signals are used to maintain synchronization of the frames, and that key numbers are embedded into the video stream following the synchronization signal, but before the frame.” *Id.* at 47 (citing Ex. 1004, 1:67–2:9 (“[D]ata transmitted . . . consists of input data D . . . the cipher key number sending section 14 and multiplexed at the multiplexing section 15, and frame synchronizing signals F.”), 6:34–39, 7:27–32, Figs. 4, 6, 17; Ex. 1003 ¶ 183). According to Petitioner, “[t]he key number is ‘multiplexed’ in a synchronized manner with encrypted data ‘D’ and ‘frame synchronizing signals F,’ *with key numbers transmitted ‘at regular intervals’* or ‘with each of frames.’” *Id.* at 48 (emphasis added) (citing Ex. 1004, 1:67–2:9, 4:55–57, Fig. 17; Ex. 1003 ¶ 183).

Petitioner further contends that “Fetkovich teaches multiplexing its encryption parameters into the video stream, embedded with associated frames.” *Id.* at 48 (citing Pet. § VI.A.2[1f]). According to Petitioner, “Fetkovich teaches the importance of maintaining ‘synchronization’ for the frame decryption process.” *Id.* (citing Ex. 1005, 7:35–50). Like Ueno, “Fetkovich teaches using a ‘signal’ to maintain the synchronization of the

frame decryption information (e.g., encryption parameters) with the sequence of frames.” *Id.* (citing Ex. 1005, 7:55–67 (“A mechanism for determining that encryption/decryption synchronization has been lost *might be to place a signal in the first unit of encryption (whether encrypted or not) after a key change .....*” (emphasis added))); Ex. 1003 ¶ 184).

According to Petitioner, “the combination of Ueno and Fetkovich renders obvious interleaving frame decryption information with synchronization signals into the video stream before the data of the corresponding video *frames*, thereby incorporating them into a single stream.” *Id.* at 48 (emphasis added) (citing Ex. 1003 ¶ 185). “A POSITA would have understood that this frame decryption information is synchronized with the set of encrypted frames into a synchronized frame decryption stream, consistent with the ’673 patent.” *Id.* at 48–49 (citing Ex. 1003 ¶ 185; Ex. 1001, 9:23–39, Fig. 9). Petitioner contends that “[a] POSITA would have understood the combination teaches an analogous structure, with *periodic frame decryption information* embedded alongside the video frames, including the *key number and partial encryption parameters* used to encrypt/decrypt associated frames.” *Id.* at 49–50 (emphasis added) (citing Ex. 1003 ¶ 185).

Petitioner contends that “[t]his combination teaches multiplexing, which a POSITA would have understood to be synonymous with interleaving in this context because both embed frame decryption information into a video stream alongside its corresponding video frames,” and therefore, renders limitation [1g] obvious. *Id.* at 50 (citing Ex. 1004, Figs. 4, 6, 17; Ex. 1003 ¶ 185).

We are persuaded by Petitioner’s contentions, the cited portions of Ueno and Fetkovich, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches limitation [1g].

*b) Analysis of Patent Owner’s Arguments*

*Patent Owner’s Arguments Concerning Benefits of the Claimed Invention*

*First*, Patent Owner contends that the ’673 patent provides “a ‘unique approach’ to protecting streaming video that . . . involves ‘bounding the resources consumed during decryption.’” PO Resp. 5 (citing Ex. 2008 ¶ 51; Ex. 1001, 3:45–48, 3:49–51, 5:25–27, 10:29–34); *see* PO Sur-Reply 10–12. Patent Owner further contends that “the invention also permits efficient decryption of partially encrypted frames using a generic decoder (such as one suitable for full-encryption systems) rather than a specialized decoder.” PO Resp. 7. Patent Owner also contends that, “[b]ecause the invention’s decryption does not depend on frame sub-structure, it can be performed before the frame enters the decoder, allowing the decoder to receive the already-decrypted stream like in full encryption systems, so generic decoders can be used with DivX-encrypted streams.” *Id.* at 9; *see* PO Sur-Reply 7–10. Patent Owner still further contends that the ’673 patent’s “partial frame encryption approach is useful in low-processing-power consumer electronic devices” “that would not otherwise possess the requisite decrypting/decoding processing power.” PO Resp. 10.

Petitioner contends, and we agree, that Patent Owner “seeks to limit the Board’s construction to specific examples in the ’673 specification” and “[e]ven if those examples had benefits, it would still be improper to limit the claims to those examples because none of the purported benefits constitute

‘clear and unmistakable’ disavowal of embodiments lacking the benefits.” Pet. Reply 12 (citing *i4i Ltd. P’ship*, 598 F.3d at 844). Even if we were to accept that all of these advantages argued by Patent Owner had evidentiary support, the argued advantages are not recited in independent claim 1 and the intrinsic record does not reflect any reason to import these advantages into the reading of the claim.

*Patent Owner’s Arguments Concerning the Claimed  
“Frame Encryption Function”*

*Second*, Patent Owner contends that Petitioner’s proposed combination does not teach or suggest the claimed “frame encryption function” because

Fetkovich’s “encryption parameters” specify portions of the frame to be encrypted based on the frame substructure being encrypted, not based on location, by layout or offset, of a portion in the frame to which encryption is applied. Furthermore, it is undisputed that *frame substructures, such as slices and macroblocks, do not in that sense have a fixed “location” in the frame*. Finally, construing “frame encryption function” to encompass Fetkovich’s encryption parameters based on frame substructure, rather than where in the frame encryption is applied, would contradict the functionality of the Patent’s embodiments and the Patent’s solution to the problem it sought to solve.

*Id.* at 23 (emphasis added) (citing Ex. 2008 ¶ 76); *see id.* at 26 (arguing that “the sub-structures cannot even be identified within the frame without initiating the process of decoding the frame”); *see* PO Sur-Reply 1–4. Patent Owner also presents arguments disputing that Fetkovich’s delay can be considered to teach the limitations of the claim. PO Sur-Reply 14–15.

Petitioner responds, and we agree, that “while bytes are used in some embodiments, the ’673 specification uses broader language of ‘unit’ and

makes clear that bytes are just one non-limiting example of the units in an encryption layout.” Pet. Reply 7 (citing Ex. 1001, 6:25–38; Ex. 1019 ¶ 23). Petitioner further persuasively argues that “[s]lices and macroblocks are common units of video data.” *Id.* at 8 (citing Ex. 1019 ¶ 25; Ex. 1006, 22:63–23:7 (“Such units may consist of . . . sub-frame units..... ”); Ex. 1005, 4:30–44 (“an MPEG stream can be described as including the following units: .....picture, slice, and macroblock”))).

Petitioner also persuasively argues that Patent Owner “concedes that Fetkovich ‘specif[ies] portions of the frame to be encrypted’ and that Patent Owner “only disputes whether [Fetkovich] specifies ‘location’ in bytes—which . . . is not required by the claims.” *Id.* at 9 (first alteration in original). Petitioner further contends that “[e]ven if [a] ‘fixed’ location were required, it is nonetheless met” because “Fetkovich teaches a delay parameter that includes a delay of zero.” *Id.* at 11 (citing Ex. 1005, 5:57–60 (“Delay . . . This number is zero-origin.”))). According to Petitioner, “encryption is applied to the first macroblock or slice of the selected frame—which has a fixed location.” *Id.*

As discussed above in Section II.A, we do not adopt Patent Owner’s construction for “frame encryption function.” That is, we determine that “frame encryption function” is not limited to being specified in data units of bytes, and the claim term does not exclude frame sub-structures such as slices and macroblocks as Patent Owner argues. *Supra* § II.A. Dr. Nielsen appears to confirm this understanding:

MR. QIU: Is it your opinion that when the claims refer to offset, offset refers to nothing more than a byte offset?

. . . .

DR. NIELSEN: I don't see any examples in the specification of offsets other than byte offsets. I don't see any other possible interpretation of offset. *But, on the other hand, the claims just say offset information, so I suppose that could be not in bytes.*

Ex. 1029, 202:19–21, 203:9–14 (emphasis added). We further find persuasive Petitioner's contention that Patent Owner "alleged the frame encryption function is satisfied by specifying the location of encrypted portions of a frame *based on slices*"—Petitioner contends "[t]hose slices (NAL units) are variable in size and not 'fixed' bytes that PO now contends are necessary." Pet. Reply 10 (citing Ex. 1025, 52, 82; Ex. 1029, 193:10–194:8). For these reasons, Patent Owner's arguments that the combination of Ueno, Fetkovich, and Demos does not teach or suggest the claimed "frame encryption function" do not undermine Petitioner's challenge.

*Third*, Patent Owner argues that the claimed "frame encryption function" "is not the same thing as an encryption transformation, such as—according to how the Petition appears to use the phrase—DES." *Id.* at 17; *see id.* at 8, 16, 20 (contending that Petitioner had made untimely arguments by "argu[ing] its Petition had all along mapped the 'frame encryption function' to the encryption transformations like DES and Fetkovich's encryption parameters"). Patent Owner explains that "the Petition simply asserted that the limitation 'in accordance with a frame encryption function' is satisfied because the encryption (like all other encryptions) is conducted using a standard transformation algorithm such as the Data Encryption Standard (DES)." *Id.* at 16 (citing Pet. 33, 35; 76–78).

We find Patent Owner's argument that Petitioner maps "frame encryption function" to conventional encryption transformations, such as DES and AES, unavailing. *See* Pet. Reply 6 n.3 (citing Ex. 1024, 24–25;

Ex. 1023, 22; Ex. 1029, 171:22–172:6) (Petitioner arguing that Patent Owner’s “infringement contentions cite AES to argue that the frame encryption function is met”). Petitioner does not map “frame encryption function” to only a conventional encryption transformation—instead, Petitioner maps “frame encryption function” to *both* encryption parameters and a conventional encryption algorithm/transformation.

In our Decision Denying Institution, we initially determined that Petitioner implicitly argued that “frame encryption function” “is met by conventional encryption algorithms such as Data Encryption Standard (DES), Triple DES, and Blowfish.” DDI 7 (citing Pet. 33–35). In our Institution Decision, however, we determined that we misapprehended Petitioner’s position and found that Petitioner’s position regarding the claimed “frame encryption function” is based on two steps—“the step of selecting what to encrypt, followed by the step of encrypting by providing the selections as input to a conventional encryption algorithm.” Inst. Dec. 4.

We maintain our determination that Petitioner’s position is based on two steps and is set forth in its Petition (and therefore, is not untimely as Patent Owner argues (PO Resp. 19–20)) because Petitioner asserts that the frame encryption function is met as follows:

The combination . . . teaches or suggests creating a set of encrypted frames . . . using the frame encryption keys in accordance with *a frame encryption function* (e.g., *using DES, Triple DES, or Blowfish to encrypt selected portions of selected frames in accordance with encryption parameters*).

. . . .  
Fetkovich teaches *encryption algorithms and encryption parameters together control the encryption process*, including the portions of the video stream to encrypt.

. . . .

Demos by itself teaches or suggests the creation of a set of encrypted frames by encrypting at least selected portions (e.g., DC coefficients or AC coefficients) of selected frames (e.g., I-frames, or I and P-frames) of said sequence of frames using the frame encryption keys in accordance with *a frame encryption function (e.g., using DES, Triple DES, or Blowfish to encrypt selected portions of selected frames)*.

Pet. 33, 35 (emphasis added) (citing Ex. 1003 ¶¶153–169; Ex. 1005, 3:4–14, 5:9–6:40). The above-quoted statements resolve or at least outweigh any ambiguity in Petitioner’s position created by the assertion in the Petition that “Ueno teaches using frame encryption keys in accordance with a frame encryption function” accompanied by a citation to Ueno’s disclosure that “[e]nciphering methods include DES . . . .” *Id.* at 35 (citing Ex. 1004, 1:13–20, 1:33–43, 4:46–59, 6:54–59; Ex. 1003 ¶ 160); *cf.* PO Resp. 16 (arguing that “Petitioner’s expert, also, simply mapped the claimed ‘frame encryption function’ to encryption transformations such as DES”), 20–21 (arguing that the “Petition argument was unambiguously that *Ueno* discloses the claimed ‘frame encryption function’ for a single reason—that it discloses utilizing the DES encryption transformation”).

In its Response, Patent Owner argues that

[t]he specification, as well as the ordinary use of this language in the art, make clear, however, that the claimed “frame encryption function” is not the same thing as an encryption transformation, such as—according to how the Petition appears to use the phrase—DES. An encryption algorithm is an algorithm (such as DES) that transforms the unencrypted data to encrypted data. In other words, the unencrypted data is fed to the transformation and the encrypted data is output from the transformation. The transformation, however, has no bearing on the layout within a frame of the encrypted data—it merely

transforms the data fed to it, wherever the data might happen to fall within the frame.

PO Resp. 17.

Petitioner responds that “[t]he ’673 specification uses DES/AES to encrypt selected portions of frames.” Pet. Reply 6 (citing Ex. 1001, 3:30–33, 8:19–30; Ex. 1019 ¶¶ 15–21). Petitioner argues that “[e]xperts for Petitioners and PO agree that an encryption algorithm is required for encrypting selected portions of frames.” *Id.* (citing Ex. 1003 ¶¶ 75, 115, 159–160; Ex. 1019 ¶ 19; Ex. 1029, 208:18–209:2).

We do not understand Petitioner’s position as being one that maps the claimed frame encryption function to *only* a conventional encryption algorithm. The background section of the ’673 patent discloses that “[v]ideo data is often encrypted using a symmetric block cipher conforming to, for example, the Data Encryption Standard (DES) or Advanced Encryption Standard (AES).” Ex. 1001, 3:31–33. The ’673 patent also discloses that

It may also be desired to apply header and offset encryption at a predetermined frequency with respect to each frame type. For example, the frequency of application of header encryption with respect to i-type frames could assume a value of ‘3’, which would mean that header offset encryption would be applied to every third frame. In particular implementations the application frequency of each type of encryption offset (i.e., header and middle offset) with respect to the various frame types can be based upon a function or series. . . . once the encryption offset has been generated and stored (step 716), sufficient information exists for the frame to be encrypted (step 718). In this regard the encryption is effected using the key previously stored (step 710) and is conducted over a specified number of units of the frame. The number of bytes encrypted may be determined based upon the level of available processing power and desired degradation of visual quality. Any type of block or stream encryption, such as encryption consistent with the Digital

Encryption Standard (DES) or Advanced Encryption Standard (AES), may be applied to the frame portion encrypted pursuant to step 718.

*Id.* at 8:5–30. Based on these cited portions of the '673 patent, we determine that the '673 patent does not exclude “conventional” encryption algorithms/transformations from performing encryption on selected frames and selected portions of these frames.

*Patent Owner’s Arguments Concerning the Claimed  
“Synchronized Frame Decryption Stream”*

*Fourth*, Patent Owner contends that Petitioner’s proposed combination does not teach or suggest the claimed “synchronized frame decryption stream.” PO Resp. 31. Specifically, Patent Owner argues that “*Fetkovich* makes clear, and the Petition does not dispute, that it transmits its encryption parameters only when the parameters are updated: in *Fetkovich* ‘[a] change in encryption method or encryption parameter may be signaled by an external signal, or the presence of something within the stream itself.’” *Id.* at 37–38 (citing Ex. 1005, 4:6–8); *accord* Pet. 51 (“Given the obviousness of sending Ueno’s key numbers with each frame, a POSITA would have similarly been motivated to multiplex Fetkovich’s encryption parameters with each frame because it facilitates Fetkovich’s goal of dynamically-changing encryption parameters.”). Patent Owner characterizes Petitioner as “argu[ing] sending encryption keys with each frame would have addressed Fetkovich’s potential synchronization problems” (*see* Pet. 51), but Patent Owner disputes that the Petition and Dr. McDaniel “explain[] how or why sending the encryption key with each frame would have ‘facilitated’ encrypting only selected frames.” PO Resp. 39 & n.7 (emphasis omitted); *see* PO Sur-Reply 20–21. Patent Owner presents similar

arguments in the context of Petitioner’s motivation to combine Ueno, Fetkovich, and Demos. In its Sur-Reply, Patent Owner contends that “Petitioner disputes Patent Owner’s construction for the first time in the Reply” and instead “now argues a ‘synchronized frame decryption stream’ does not require a 1:1 correspondence” and that the “new position is untimely.” PO Sur-Reply 16 (citing Pet. Reply 15, 24–25); *see id.* at 17–18, 21–26.

Petitioner responds, as set forth above, that Patent Owner “stated in district court that frame decryption information is *synchronized* with encrypted frames by *interleaving* the information with corresponding frames, e.g., as opposed to appending the information after all video frames.” Pet. Reply 14 (citing Pet. 50; Ex. 1011 ¶ 276 (“Netflix *synchronizes* the frame decryption information by *interleaving* the PIFF Sample Encryption Boxes (uuid) and media data, or ‘mdat,’ boxes throughout the MP4 file.”)).

As discussed above in Section II.B, we did not construe “synchronized frame decryption stream” to require sending frame decryption information in a 1:1 correspondence with each frame. Instead, we determined above that “Petitioner’s position that ‘synchronized frame decryption stream’ encompasses *providing* ‘one chunk of decryption data to correspond to several frames’ is consistent with the disclosures of the ’673 patent.” Pet. Reply 25. As set forth above, we are persuaded by Petitioner’s explanation that “[w]hen keys/parameters are only sent when changed, that ‘decryption information is used to decrypt each frame’ until ‘the last frame before new encryption parameters are received.’” *Id.* (citing Ex. 1003 ¶ 175; Pet. 42).

Patent Owner's arguments are not responsive to Petitioner's showing and accompanying motivation to combine concerning sending a key or frame decryption information *periodically*. Patent Owner's position is also at odds with the position taken in its amended district court complaint. *See* Ex. 1011 ¶ 276. For the foregoing reasons, Patent Owner's arguments as to why the combination, and Petitioner's challenge, does not teach or suggest sending frame decryption information with *each* frame are unavailing.

We also find unavailing Patent Owner's argument that Petitioner's implicit construction arguments concerning periodically sending keys or sending keys for a chunk of data is untimely. Petitioner presented this position *also* in the Petition, as we discuss above in Sections III.A.4.a and III.A.4.b.

*Fifth*, Patent Owner argues that “[t]he Petition then seems to assume that interleaving the encryption key in between frames would result in a synchronized frame decryption stream,” but “Petitioner’s proposed motivation to modify *Fetkovich* discussed in the preceding sections would only apply in a lossy rather than lossless transmission system, and in a lossy transmission system, interleaving the keys between frames does not synchronize them with the frames.” PO Resp. 56; *see* PO Sur-Reply 18–19.

Petitioner responds, and we agree, that, “the challenged claims do not mention channels at all,” “[n]or does the specification say anything about networking protocols, packets, or channels, either lossy or lossless,” and accordingly, “synchronization cannot include requirements about network delivery or packet ordering.” *See* Pet. Reply 16. For this reason, Patent Owner's argument as to interleaving and lossy/lossless transmission systems are unavailing.

*c) Petitioner's Motivation to Combine*

Petitioner contends that “Fetkovich teaches encryption parameters for dynamically controlling the portions of video frames that are encrypted, including sub-frame granularities such as slices and macroblocks,” “which were ‘granularities for MPEG video data[,]’” “the most popular video standards of the early 2000s.” Pet. 23 (alteration in original) (citing Ex. 1005, 3:4–14, 5:29–37); *see id.* (citing Ex. 1003 ¶ 127). According to Petitioner, partially encrypting video data, including by encrypting slices and macroblocks, “can render frames ‘almost impossible to comfortably view.’” *Id.* at 23–24 (citing Ex. 1005, 5:29–37, 3:15–40). Petitioner contends that Fetkovich’s partial encryption, at sub-frame granularities, “reduces computational requirements while impeding piracy, providing flexible, fine-grain control for the level of security and computation limitations of target platforms, with a scalable mechanism for encrypting selected frames at ‘different levels of thoroughness’ for different priority levels.” *Id.* at 24 (citing Ex. 1005, 3:15–39; Ex. 1003 ¶ 127).

Petitioner takes the position that a “POSITA would . . . have been motivated to apply Fetkovich’s partial encryption teachings to selected frames, rather than every frame” and cites Demos for teaching how to select which particular frames are to be encrypted. *Id.* (citing Ex. 1003 ¶ 128). Petitioner ties Demos into the teachings of Fetkovich, noting that, like Fetkovich, Demos acknowledges the confounding effect of encrypting “[s]ub-units of frames,” instead of an entire frame. *See* Ex. 1006, 23:38–43, Table 8.

Petitioner contends that Demos teaches encrypting only I and P frames due to their “high influence,” which is thus “better for encryption.”

Pet. 25 (citing Ex. 1006, 22:53–58, 23:8–24:18, Fig. 11; Ex. 1003 ¶ 130). “Encrypting only I and P frames provides a large reduction in computational load *while maintaining protection for all frames*; a POSITA would have found this advantageous and been motivated to pursue it.” *Id.* (emphasis added). Thus, Petitioner contends that Demos “allows partial encryption of potentially arbitrary selection of frames, such as important scenes.” Pet. 26 (citing Ex. 1003 ¶ 132).

Petitioner contends that, “[g]iven Demos’ and Fetkovich’s teachings, a POSITA would have been motivated to use three obvious selections of frames for partial encryption: (1) I and P frames; (2) every other minute of frames; or alternatively, (3) frames of particularly important plot or action scenes.” *Id.* at 25 (citing Ex. 1003 ¶ 131).

In Petitioner’s view, both Fetkovich and Demos “provide substantial content protection with reduced computational requirements.” *Id.* at 24–25 (citing Ex. 1003 ¶ 129). Petitioner further contends that “[b]eyond Fetkovich’s benefits, this combination would have additional computational savings by customizing the level of encryption based on the video content and frames,” a benefit expressly disclosed by Fetkovich. *Id.* at 26 (citing Ex. 1003 ¶ 131), 24 (citing Ex. 1005, 4:30–65).

Petitioner contends that “Demos and Fetkovich teach that keys should be changed and Ueno provides an elegant, widely-known mechanism for doing so.” *Id.* at 19 (citing Ex. 1003 ¶ 113; Ex. 1006, 24:42–49; Ex. 1005, 3:60–4:5). According to Petitioner, “Fetkovich teaches its encryption parameters may include an encryption key” and that “[w]hen combined with Ueno, a POSITA would have been motivated to send key numbers, as taught by Ueno, instead of actual keys . . . .” *Id.* at 21 (citing Ex. 1005, 3:7–10,

7:18–22; Ex. 1003 ¶ 118). Petitioner contends that “Ueno’s teachings facilitate key changes, which makes cryptographic attacks more difficult and limits the impact if a key is compromised.” *Id.* (citing Ex. 1004, 2:50–53; Ex. 1003 ¶ 116). “Ueno changes keys by sending key numbers, rather than keys themselves, and it allows returning to previous keys in the table, which can be advantageous with frequent key changes.” *Id.* (citing Ex. 1003 ¶¶ 114, 116). “Key tables were widely used to store and organize keys, correlated to key identifiers, which were commonly used to specify the keys used to encrypt/decrypt data.” *Id.* (citing Ex. 1003 ¶¶ 114, 117).

Petitioner contends that “[a] POSITA would have been motivated to interleave Ueno’s key number with Fetkovich’s encryption parameters into the video stream, including for each video frame.” Pet. 20 (citing Ex. 1004, 1:37–42, Figs. 4, 6, 17; Ex. 1005, 6:57–61; Pet. §§ VI.A.2[1f–1g]); *see also id.* at 21 (citing Ex. 1003 ¶¶ 115, 117; Pet. § VI.A.2[1g]) (Petitioner also contending that “a POSITA would have been motivated to apply Ueno’s teachings regarding key tables and interleaving the active key number within the video stream, including for every frame”). Petitioner further contends that “Ueno’s framework maintains and restores synchronization, for example by multiplexing key numbers into the video stream, including for each frame, which automatically restores synchronization with every frame.” *Id.* at 23 (citing Ex. 1004, 1:32–42, 2:5–9, Fig. 16; Ex. 1003 ¶ 124).

*d) Analysis of Petitioner’s Challenge*

As discussed in Section II.B, we are persuaded by Petitioner’s second alternative position in which Petitioner implicitly construes “synchronized frame decryption stream” to allow “*one chunk* of decryption data to correspond to *several frames*.” Pet. Reply 24–25 (emphasis added).

Petitioner explains, and we are persuaded, that “[w]hen keys/parameters are only sent when changed, that ‘decryption information is used to decrypt each frame’ until ‘the last frame before new encryption parameters are received.’”

*Id.* (citing Ex. 1003 ¶ 175; Pet. 42). As we do not determine that “synchronized frame decryption stream” requires “a 1:1 synchronized correspondence between decryption information and an encrypted frame,” (*supra* § II.B; PO Sur-Reply 16), we need not rely on Petitioner’s first alternative position in which Petitioner implicitly construes the term to require the sending of “frame decryption information” with *each* frame.

We are persuaded by Petitioner’s motivation to combine based on the contentions set forth above in Section III.A.4.c, which we agree are supported by the cited portions of Fetkovich, Demos, and Ueno and Dr. McDaniel’s testimony so as to establish sufficient rational underpinnings. We highlight certain contentions and disclosures cited by Petitioner below.

Fetkovich discloses that “an MPEG stream may be transmitted using varying levels of encryption depending upon the sensitivity of the video material.” Pet. 24 (quoting Ex. 1005, 4:61–63). Specifically, Fetkovich discloses that “an MPEG stream can be described in the following units: program, sequence, group of pictures (GOPs), picture, *slice*, and *macroblock*” and that “dynamic encrypting can occur at any one of these levels.” Ex. 1005, 4:38–42 (emphasis added). Demos operates in a manner similar to that of Fetkovich and teaches partial encryption that works on selected frames because it discloses that, in order “to protect a work commercially, not every unit need by [sic] encrypted or confounded by the encryption of a higher-level unit.” Pet. 24 (quoting Ex. 1006, 22:39–41).

We are persuaded that Fetkovich expressly motivates the combination with Demos because Fetkovich discloses encrypting selected frames instead of all of them—Petitioner contends, and we agree, “Fetkovich’s density parameter . . . control[s] the percentage of encrypted units and . . . signal[s] when the frame is not encrypted with a density of 0.” *Id.* at 26 (citing Ex. 1005, 5:28–6:40; Ex. 1003 ¶¶ 131–132).

Demos also expressly motivates a combination with Fetkovich’s partial encryption at sub-frame granularities because Demos discloses that “an entire frame need not be encrypted to confound some or all of a [Group of Pictures (‘GOP’)]” because “[s]ub-units of frames may be encrypted and still have a confounding affect [sic], while reducing encryption and decryption processing time.” Ex. 1006, 23:37–40 (emphasis added). Like Fetkovich, Demos discloses partial encryption based on, for example, sensitivity, of the subject matter of a content stream—“a film may be rendered worthless to pirates if every other minute of film, frames or particularly important plot or action scenes are encrypted or confounded.” *Id.* at 22:41–44.

Accordingly, we are persuaded that the combination of Fetkovich and Demos teaches varying degrees of encryption by partially encrypting selected frames at selected sub-frame granularities, thus providing computational resource savings and customizable security depending on the sensitivity and/or security requirements of the subject matter of the content stream.

We are also persuaded that Fetkovich motivates a combination with Ueno as Fetkovich discloses that “its encryption parameters may include an encryption key” (Pet. 21 (citing Ex. 1005, 3:7–10, 7:18–22)) and Ueno

discloses that “input data D enciphered by the data enciphering section 11, the cipher key number N(ks) output from the cipher key number sending section 14 and multiplexed at the multiplexing section 15, and frame synchronizing signals F.” Ex. 1004, 2:1–5. Ueno also discloses that “[t]he cipher key number N(ks) is usually transmitted *only when it has been changed*; in some cases, the cipher key number is transmitted *at the start of data communication* or *at regular intervals*, or is transmitted with each of frames.” *Id.* at 2:5–9 (emphasis added). Thus, we are persuaded that “[a] POSITA would have been motivated to interleave Ueno’s key number with Fetkovich’s encryption parameters into the video stream . . . .” Pet. 20 (citing Ex. 1004, 1:37–42, Figs. 4, 6, 17; Ex. 1005, 6:57–61; Pet. §§ VI.A.2[1f–1g]). As such, we find Petitioner’s motivation to combine Ueno and Fetkovich sufficiently supported by rational underpinnings.

Petitioner asserts that “[a] POSITA would have had a reasonable expectation of success when combining the reference[s’] teachings because they were well-known aspects of video streaming, used for their known purposes in a complimentary manner.” *Id.* at 27 (citing Ex. 1003 ¶ 139); *id.* at 27–28 (citing Pet. §§ I, IV; Ex. 1009, 1:49–63, 2:1–8, 8:23–32; Ex. 1003 ¶¶ 139–140; Ex. 1004, 1:21–22). Petitioner further contends, and we agree, that

[a] POSITA would have found the combination to be routine, predictable, and well within the level of ordinary skill. The references are directed to similar techniques. Fetkovich and Demos both teach partial encryption based on “units” including frames, slices, and macroblocks. *See* Fetkovich and Ueno teach similar, flexible frameworks for dynamically changing encryption parameters including by multiplexing parameters into the video stream.

The alleged invention is a combination of familiar elements (e.g., partial video encryption, key tables, and multiplexed encryption information) according to known methods (e.g., partially encrypting video using a key table and then multiplexing encryption information into the video stream) to yield predictable results (e.g., a partially-encrypted streaming video system with decryption information).

*Id.* at 28 (citing *KSR*, 550 U.S. at 401; Ex.1003 ¶¶ 140–142; Ex. 1004, 1:67–2:9; Ex. 1005, 3:4–14, 5:29–33, 6:49–65, Figs. 1, 2; Ex. 1006, 23:8–24:18, Fig. 11). Petitioner contends, and we are persuaded, that “[a]ll of these components were already used for streaming video years before the ’673 patent.” *Id.*

For all of the foregoing reasons, we are persuaded that one of ordinary skill in the art would have been motivated to combine Ueno, Fetkovich, and Demos as proposed by Petitioner and would have had a reasonable expectation of success in so doing.

*e) Objective Indicia of Non-Obviousness*

Objective indicia of nonobviousness (also referred to as secondary considerations) may include long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, industry praise, and expert skepticism. *Mintz v. Dietz & Watson, Inc.*, 679 F.3d 1372, 1379 (Fed. Cir. 2012). Objective indicia are “only relevant to the obviousness inquiry ‘if there is a nexus between the claimed invention and the [objective indicia of nonobviousness].’” *In re Affinity Labs of Tex., LLC*, 856 F.3d 883, 901 (Fed. Cir. 2017) (quoting *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1312 (Fed. Cir. 2006)); *see also ClassCo, Inc. v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016). As the Federal Circuit explained, “a patentee is entitled to a rebuttable presumption of nexus between the

asserted evidence of secondary considerations and a patent claim if the patentee shows that the asserted evidence is tied to a specific product and that the product ‘is the invention disclosed and claimed.’” *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019), *cert. denied*, 141 S. Ct. 373 (2020) (quoting *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)). That is, presuming nexus is appropriate “when the patentee shows that the asserted objective evidence is tied to a specific product and that product ‘embodies the claimed features, and is coextensive with them.’” *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). On the other hand, the patentee is not entitled to a presumption of nexus if the patented invention is only a component of a commercially successful machine or process. *Id.* (reaffirming the importance of the “coextensiveness” requirement).

Applying *Fox Factory*, the Board uses a two-step analysis in evaluating nexus between the claimed invention and the evidence of secondary considerations. *Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020) (precedential). We first consider whether a patent owner has demonstrated “that its products are coextensive (or nearly coextensive) with the challenged claims,” resulting in a rebuttable presumption of nexus. *Id.* at 33.

Here, as Petitioner correctly argues, Patent Owner “introduces evidence of DivX’s products but does not argue secondary considerations or make any effort to argue nexus.”<sup>6</sup> Pet. Reply 26. Petitioner further argues

---

<sup>6</sup> Patent Owner did not characterize any of the arguments or evidence presented in its Patent Owner’s Response as objective indicia of non-obviousness and only did so when questioned during oral argument. *See* Tr.

that Patent Owner “is not entitled to a presumption of nexus when the claimed features constitute a small part of the claimed product and are far from coextensive.” *Id.* Patent Owner asserts and Dr. Nielsen testifies that “DivX implemented its inventive partial encryption [method or approach] into DivX’s Digital Right Management Systems” and each cite to Exhibit 2020, a claim chart comparing challenged claims 1, 2, 4, 5, 10, 14, and 17–19 of the ’673 patent to features of DivX’s Decoder Software Development Kit (SDK). PO Resp. 11; Ex. 2008 ¶ 61. Patent Owner does not assert or explain that it is arguing secondary considerations of non-obviousness, does not attempt to establish a nexus between the claimed features and Patent Owner’s commercial product, and does not discuss or explain Exhibit 2020 in *any* level of detail. *See generally* PO Resp.; *see also* Pet. Reply 26 n.15 (citing Ex. 1029, 131:25–132:20) (Petitioner arguing that “Exhibit 2020 was not prepared by an expert witness or discussed in briefing”). For these reasons, we determine that a presumption of nexus is inappropriate here—Patent Owner does not provide an analysis demonstrating that its product(s) are coextensive (or nearly coextensive) with the challenged claim. *See Lectrosonics*, Paper 33 at 33. As such, we proceed to the second step of the analysis under *Fox Factory*.

Even without the presumption, a patent owner “is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention,’” in the second step of the analysis. *Fox Factory*, 944

---

72–77 (Patent Owner’s counsel responding to the panel’s questioning on whether Patent Owner intended to argue secondary considerations or nexus in its briefing).

F.3d at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). Also, the nexus must be “to some aspect of the claim not already in the prior art.” *In re Kao*, 639 F.3d 1057, 1069 (Fed. Cir. 2011). Once a patent owner has presented a prima facie case of nexus, the burden of coming forward with evidence in rebuttal shifts to the challenger to adduce evidence showing that the objective indicia was due to extraneous factors other than the patented invention. *Demaco*, 851 F.2d at 1392–93. “Ultimately, the fact finder must weigh the [objective indicia] evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan.” *Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331–32 (Fed. Cir. 2016)).

Patent Owner presents evidence of secondary considerations that appears to generally address at least: industry-wide praise and/or licensing; commercial success; and failure of others. With regard to the second step of the analysis under *Fox Factory*, Patent Owner’s evidence of secondary considerations is not shown to be the “direct result of the unique characteristics of the claimed invention” and Patent Owner does not prove nexus without the presumption, for the reasons discussed below. *Fox Factory*, 944 F.3d at 1373–74.

Patent Owner contends that the ’673 patent discloses a “unique approach to partial frame encryption” that is “incorporated into DivX’s Digital Rights Management (‘DRM’) [product] [and] licensed and adopted for video codecs around the world.” PO Resp. 1 (citing Ex. 2006, 1–2; PO Resp. § 2). Patent Owner asserts that DivX’s DRM product, using the partial frame encryption method taught by the ’673 patent, has been deployed in over one billion consumer devices, protects over 43,000

professional titles, and that “major consumer electronics manufacturers such as LG and Samsung have paid hundreds of millions of dollars to license DivX’s Software Development Kit, including this DRM [product] practicing the invention.” *Id.* (citing Ex. 2006, 1–2); *see also id.* at 11 (citing Ex. 2006, 2–3). Exhibit 2006 is a document describing DivX’s revenue growth for certain categories of licensing, the size of its customer base, particularly in terms of usage and installation, and the size of its content library, as well as general areas of predicted expansion or growth. At its most specific, Exhibit 2006 describes the number of files protected by DRM, DRM content delivery, and the deployment and adoption of DRM. Neither Exhibit 2006 nor Patent Owner’s arguments explain how we might interpret this document to show, for example, that its licensing activity is due to the particular portion of DRM that specifies the claimed partial frame encryption invention. Stated differently, there is insufficient support for the proposition that consumer electronics manufacturers, including LG, Samsung, or any other entity, licensed DivX’s DRM product *because of* the partial frame encryption method recited in the claims. If indeed the invention(s) claimed in the ’673 patent is/are incorporated in the DRM that is included in DivX’s Software Development Kit, there is no evidence that any of the installation, deployment, and growth numbers are due to the claimed partial frame encryption invention of claim 1 (or any other challenged claim).

Patent Owner contends that “prior to the claimed invention there was a string of failed attempts to achieve efficient access protection without fully encrypting compressed video” and cites a 1996 “IEEE experimental study” that “tested, and rejected, numerous ‘previously proposed selective

encryption schemes for MPEG video security.” PO Resp. 3–4 (citing Ex. 2017, 1–5).<sup>7</sup> According to Patent Owner, “DivX players achieved wide adoption because they could be used on codecs utilizing limited-power consumer device processors of the time, where the processing demands of decrypting the DivX encrypted frames could be restricted so as not to exceed these components’ ‘peak processing power.” *Id.* at 6 (citing Ex. 1001, 10:29–34; PO Resp. § II.C); *see also id.* at 6 (citing Ex. 2017, 8); *id.* at 8 (citing Ex. 2017, 3).

As to Patent Owner’s purported evidence of failure of others, Petitioner contends that “PO only considers a single paper from 1996 (Agi, Ex. 2017), shortly after the development of partial encryption was kickstarted by a famous 1995 paper (Spanos and Maple).” Pet. Reply 27 (citing Ex. 1003 ¶ 67; Ex. 1008). Petitioner asserts that “[b]y 2002, POSITAs knew many partial encryption techniques.” *Id.* (citing Ex. 1003 ¶ 68; Ex. 1007; Ex. 1009). According to Petitioner, Patent Owner “did not consider the developments in the six years after [the] Agi [Study]” and “did not dispute, or even address, that a POSITA knew how to use partial encryption in 2002.” *Id.* (citing Pet. 17).

In the Agi Study, the authors “conducted an experimental study of . . . proposed selective encryption schemes for MPEG video security.” Ex. 2017, Abstract. The authors determined that the studied selective encryption schemes “were inadequate for sensitive applications.” *Id.* The paper discusses “the tradeoffs between levels of security and computational

---

<sup>7</sup> Exhibit 2017 (“Agi Study”) is a paper by Agi et al., “An Empirical Study of Secure MPEG Transmission” in the *ISOC Symposium on Network and Distributed System Security*, San Diego, CA (Feb. 1996).

and compression efficiency.” *Id.* In the study, the authors studied “a selective encryption algorithm [that] encrypts only I-frames of MPEG video.” *Id.* at 3. The authors determined that “MPEG video cannot be secured by simply encrypting the encoded I-frames.” *Id.* at 5. But they also determined that “simple selective encryption may be sufficient for certain applications, such as cable television broadcast of pay channels, where quality of service supersedes high security as the driver.” *Id.* The authors also experimented with encrypting I-blocks along with I-frames, as well as encrypting P-frames. *Id.* The authors sought to improve security, for example, “by increasing the I-frame frequency” at the expense of “increased video size, a higher network bandwidth consumption, and higher computational complexity for encryption and decryption.” *Id.* at 8.

While the Agi Study explains the tradeoffs between security and resources consumed, it does not indicate that selective encryption does not work, or fails, when applied to frames and/or blocks of MPEG video. Although the studied selective encryption techniques were insufficiently secure for some applications (e.g., presentations on business finances), they were sufficiently secure for less sensitive applications (e.g., pay-per-view television)—the selective encryption techniques did not fail for all applications. As such, we do not discern that Exhibit 2017 evidences a failure that would tend to support Patent Owner’s arguments concerning non-obviousness. We also are persuaded by Petitioner’s arguments that Patent Owner’s discussion and Exhibit 2017 are not contemporaneous with the earliest priority date of the ’673 patent. Patent Owner does not present evidence that selective encryption techniques were stagnant in the six

intervening years between the publication of the Agi Study in 1996 and the earliest possible priority date of the '673 patent, 2002.

Patent Owner contends that “DivX implemented its inventive partial encryption approach into DivX’s Digital Right Management Systems,” and that “DivX developer kits specifically highlighted the invention’s benefits, touting for example the fact that developers could cap the processing power needs of a DivX encrypted video based on manufacturer limits.” PO Resp. 11 (citing Ex. 2008 ¶ 61; Ex. 2020; Ex. 2004, 1267 (“Amount of decryption is bounded and deterministic to give consistent and low performance overhead.”)); *see* Ex. 2004, 1280. Patent Owner asserts that the benefit of capping processor power needs “was possible because DivX’s method could specify, *e.g.*, the layout and offset of bytes encrypted in each frame, unlike partial encryption schemes like those in *Fetkovich* and *Demos*.” PO Resp. 11. According to Patent Owner, “DivX developer kits also highlighted that DivX DRM could be used by components already in devices.” *Id.* (citing Ex. 2005, 1248 (“technology provided by the SDK is intended to be ported to an embedded environment or consumer device”)).

Exhibit 2004, which describes DivX’s DRM Software Development Kit, lists that the “[a]mount of decryption is bounded and deterministic to give consistent and low performance overhead” in a list of fourteen “Requirements and Parameters.” Ex. 2004, 1666–67. It also states that “DivX Certification defines the configuration of AES” and “defines how much of [a] frame is to be encrypted.” *Id.* at 1280. Exhibit 2004 further states that “[i]t is a fixed amount for each frame, which keeps processing bounded and consistent.” *Id.* Even if any of the quoted “Requirements and Parameters” or “benefits” are due solely to the claimed partial frame

encryption method of the '673 patent, there is no evidence that consumers or users of the SDK purchased, licensed, or used the DRM product because of these particular benefits. For example, users may have purchased or used the product due to any other of the fourteen "Requirements and Parameters." Exhibit 2005, which describes DivX's Decoder SDK, states that the "technology provided by the SDK is intended to be ported to an embedded environment or consumer device." Ex. 2005, 1248. Similarly, it is not clear how this statement relates to the claimed partial frame encryption method. To the extent the quoted statements in Exhibits 2004 and 2005 could be considered praise, they are not supportive of Patent Owner's position because they constitute self-serving praise, if they can be considered that, and not industry-wide praise, from peers or leaders in similar industries.

For the reasons discussed above, we are not persuaded that Patent Owner has met its burden to establish a nexus between the claimed invention and the submitted evidence relating to industry-wide praise and licensing, commercial success, as well as failure of others. Absent a nexus, we determine that Patent Owner's evidence of objective indicia does not weigh in favor of non-obviousness.

*f) Weighing the Graham Factors*

"Once all relevant facts are found, the ultimate legal determination [of obviousness] involves weighing of the fact findings to conclude whether the claimed combination would have been obvious to an ordinary artisan."

*Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1361 (Fed. Cir. 2017). Above, based on full record before us, we provide our factual findings regarding (1) the level of ordinary skill in the art, (2) the scope and content of the prior art, (3) any differences between the claimed

subject matter and the prior art, and (4) objective evidence of nonobviousness.

In particular, we find that (1) Petitioner’s proposed level of ordinary skill in the art is consistent with the prior art of record (*supra* § I.h); (2) Ueno, Fetkovich, and Demos teach each of the limitations of independent claim 1 (*supra* § III.A.4.a); (3) one of ordinary skill in the art would have had a reason with rational underpinning to combine Ueno, Fetkovich, and Demos and would have had a reasonable expectation of success in so doing (*supra* §§ III.A.4.c, III.A.4.d); and (4) there is insufficient demonstration of nexus to objective evidence of nonobviousness in the record (*supra* § III.A.4.e).

Weighing these findings with our determinations of the level of ordinary skill and objective evidence of nonobviousness in the record, a preponderance of the evidence persuades us that independent claim 1 of the ’673 patent is unpatentable over Ueno, Fetkovich, and Demos.

## 5. *Independent Claim 14*

### a) *Petitioner’s Element-by-Element Analysis*

With respect to claim 14 and its recitation of “frame decryption function,” Petitioner primarily relies on its analysis with respect to claim 1 as to how the combination of Ueno, Fetkovich, and Demos teaches or suggests the “frame encryption function.”

*[14a] A method for decrypting a protected stream of compressed video content comprising:*

Petitioner contends that “Demos teaches a method for decrypting . . . a protected stream of compressed video content.” Pet. 68 (citing Ex. 1006, 28:10–13; Ex. 1003 ¶ 235). Petitioner further contends that Fetkovich

“teaches decrypting a protected stream of compressed video content.” *Id.* (citing Ex. 1005, 2:11–12, 6:66–7:7, Fig. 1; Ex. 1003 ¶ 236). Having reviewed the cited portions of Demos and Fetkovich and the accompanying testimony of Dr. McDaniel, we are persuaded that the combination of Ueno, Fetkovich, and Demos—in particular, Demos and Fetkovich—teaches the subject matter of the preamble of claim 14. We need not determine whether the preamble is limiting as Petitioner sufficiently shows that the combination teaches the subject matter of the preamble.

*[14b] receiving an input stream of compressed video content containing encrypted frames and unencrypted frames;*

Petitioner contends that “Ueno teaches sending the protected stream to a receiver, which therefore receives an input stream of compressed video content containing encrypted frames and unencrypted frames.” Pet. 70 (citing Ex. 1004, 4:20–30, 1:44–52, 4:60–5:14, 6:60–67, Figs. 1, 2, 5, 16; Ex. 1003 ¶ 239).

Petitioner further contends that “Demos . . . teaches decrypting the protected stream of compressed video content by an authorized decryption system, which obviously receives an input stream of compressed video content containing encrypted and unencrypted frames.” *Id.* (citing Ex. 1006, 28:10–13, 3:25–30). According to Petitioner, “[a] POSITA would have found it obvious that the authorized decryption system (e.g., a client) first receives the protected video stream before it can decrypt it.” *Id.* (citing Ex. 1003 ¶ 240).

Petitioner still further contends that “Fetkovich further teaches that a receiver receives the protected stream of video content.” *Id.* at 71 (citing Ex. 1005, 6:66–7:7, Fig. 1; Ex. 1003 ¶ 241); *see id.* (citing Ex. 1003 ¶ 242).

We are persuaded by Petitioner’s contentions, the cited portions of Ueno, Demos, and Fetkovich, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches limitation [14b].

*[14c] receiving frame decryption information necessary to decrypt said encrypted frames, said frame decryption information is synchronized with said set of encrypted frames into a synchronized frame decryption stream and distinguishes said encrypted frames from said unencrypted frames;*

Petitioner contends that the combination of Ueno, Fetkovich, and Demos “teaches or suggests that the synchronized frame decryption stream includes encryption status information corresponding to each frame of said protected stream, which indicates whether each frame is encrypted or not . . . and thereby distinguishes the encrypted frames from the unencrypted frames of the protected stream.” Pet. 72 (citing Pet. § VI.A.4; Ex. 1003 ¶ 244).

Petitioner alternatively contends Demos

teaches that the frame decryption information distinguishes encrypted frames from unencrypted frames to aggregate a number of similar encrypted portions (e.g., DC or AC coefficients) and decrypt them as a group, “for an entire frame” which can facilitate parallel decryption. To do so, a POSITA would have found it obvious to utilize information identifying encrypting frames and portions of frames, which distinguishes encrypted frames from unencrypted frames. Attempting decryption without this type of information would have been computationally infeasible for video streaming; thus Demos renders this limitation obvious.

*Id.* (citing Ex. 1006, 24:20–40, 25:31–35; Ex. 1003 ¶¶ 245, 246). According to Petitioner “Demos teaches partially encrypting selected video frames, including encrypting every other minute or potentially arbitrary selections such as frames from important scenes,” and that, “[t]o decrypt such a video,

it would have been obvious for the frame decryption information to distinguish encrypted from unencrypted frames with encryption status information.” *Id.* at 73 (citing Pet. §§ VI.A.4, VI.A.1, VI.A.2[1d]; Ex. 1006, 22:29–44; Ex. 1003 ¶ 247).

We are persuaded by Petitioner’s contentions, the cited portions of Demos, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches limitation [14c].

*[14d] obtaining an applicable frame decryption key from the received frame decryption information; and*

Petitioner contends that “Ueno further teaches extracting the key number from the received frame encryption information and using it to obtain the key that was used to encrypt the particular frame.” Pet. 73 (citing Ex. 1004, 1:44–52). Petitioner further contends that “[t]he combination teaches the use of symmetric encryption, meaning the encryption key is also the decryption key.” *Id.* at 74 (citing Pet. § VI.A.5 (claim 4); Ex. 1001, 8:62–67, Fig. 8 (step 830)); *see id.* (citing Ex. 1003 ¶¶ 249, 250).

We are persuaded by Petitioner’s contentions, the cited portions of Ueno, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches limitation [14d].

*[14e] decrypting selected portions of said encrypted frames using a frame decryption function in accordance with said frame decryption information, which identifies the specific portions of the frames to be decrypted and the applicable frame decryption key from the frame decryption information.*

Petitioner contends that Ueno, Fetkovich, and Demos teach “the inverse operation of decrypting the selected (encrypted) portions of encrypted frames using frame decryption information that identifies the

specific portions of the frames to be decrypted (e.g., through the encryption parameters) and the applicable frame decryption key (e.g., through the key number).” Pet. 76–77 (citing Ex. 1005, 6:66–7:7, 2:23–42, 3:4–15; Pet. § VI.A.1; Ex. 1003 ¶ 252). Petitioner further contends that “[e]ncryption parameters for granularity, density scale, density, and delay control the partial encryption process and identify the specific portions of the frames that are encrypted—and thus need to be decrypted.” *Id.* at 77 (citing Pet. § VI.A.2[1d] (explaining Fetkovich’s encryption parameters); *see id.* (citing Ex. 1005, 6:24–40; Ex. 1003 ¶ 253)).

Petitioner alternatively contends that “Ueno teaches decrypting the encrypted frames using frame decryption information that includes a key number identifying the applicable frame decryption key.” *Id.* (citing Ex. 1004, 1:44–52 (“The receiver 2 includes a separating section 21 for . . . separating the received data into enciphered data and a cipher key number, . . . and a data deciphering section 24 for *deciphering the separated enciphered data by means of a cipher key ks specified by the cipher key number N(ks)*’.” (emphasis added)), 1:67–2:9, 5:33–44, 4:60–5:14, 6:60–67, Figs. 1, 2, 5, 16).

As yet another alternative, Petitioner contends that “Demos further renders this limitation obvious.” Pet. 78 (citing Ex. 1006, 28:10–13 (“For decompression, *the relevant key(s) would be applied to decrypt the data stream.*” (emphasis added)), 25:31–35; Ex. 1003 ¶ 255); *see id.* (citing Pet. §§ VI.A.1, VI.A.2[1c-1d], VI.A.11[14d]; Ex. 1003 ¶¶ 254–256).

According to Petitioner, “[t]he references further teach decrypting selected portions of encrypted frames using a frame decryption function in accordance with the frame decryption information,” and that, as an example,

“the references teach using symmetric algorithms for decrypting the selected portions of encrypted frames in accordance with the frame decryption information, as explained above.” *Id.* at 78 (citing Ex. 1003 ¶ 257; Ex. 1004, 1:16–20; Ex. 1005, 6:52–56; Ex. 1006, 27:65–28:1; Pet. §§ VI.A.1, VI.A.5 (claim 4)).

We are persuaded by Petitioner’s contentions, the cited portions of Ueno, Demos, and Fetkovich, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches limitation [14e].

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claim 14 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

*b) Weighing the Graham Factors*

Based on full record before us, we provide our factual findings regarding (1) the level of ordinary skill in the art, (2) the scope and content of the prior art, (3) any differences between the claimed subject matter and the prior art, and (4) objective evidence of nonobviousness. Similar to our discussion above in Section III.A.4.f with respect to independent claim 1, we find that (1) Petitioner’s proposed level of ordinary skill in the art is consistent with the prior art of record (*supra* § I.H); (2) Ueno, Fetkovich, and Demos teach each of the limitations of independent claim 14 (*supra* § III.A.5.a); (3) one of ordinary skill in the art would have had a reason with rational underpinning to combine Ueno, Fetkovich, and Demos would have had a reasonable expectation of success (*supra* §§ III.A.4.c, III.A.4.d); and

(4) there is insufficient demonstration of nexus to objective evidence of nonobviousness in the record (*supra* § III.A.4.e).

Weighing these findings with our determinations of level of ordinary skill and objective evidence of nonobviousness in the record, a preponderance of the evidence persuades us that independent claim 14 of the '673 patent is unpatentable over Ueno, Fetkovich, and Demos.

Our weighing of the *Graham* factors set forth in this Section and in Section III.A.4.f applies to dependent claims 2–6, 9, 10, 13, and 15–19 and is adopted, but not repeated, in Sections III.A.6–III.A.12.

#### 6. *Dependent Claim 2*

Claim 2 depends from claim 1 and further recites “wherein said synchronized frame decryption stream includes references to frame encryption keys in the key table.” Ex. 1001, 11:61–63.

Petitioner contends that “Ueno teaches generating frame decryption information that includes key numbers that are references to frame encryption keys stored in the key table.” Pet. 52 (citing Ex. 1004, 1:53–57, 1:43–52, 5:15–32, 4:45–49, 6:54–59). Petitioner also contends “Ueno further teaches that a receiver of a data stream identifies a key to be used to decrypt a portion of the data stream based on the key number accompanying the data stream.” *Id.* (citing Ex. 1004, 1:57–64, 5:39–44, 6:60–67). Petitioner that, accordingly, “[i]t would have been obvious for these keys to be used for partially encrypting video frames, and thus a POSITA would have understood them to be frame encryption keys stored in the key table.” *Id.* at 53 (citing Pet. §§ VI.A.2[1c-1d], VI.A.1).

We are persuaded by Petitioner’s contentions and the cited portions of Ueno that the combination of Ueno, Fetkovich, and Demos teaches the limitation recited in claim 2.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claim 2 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

7. *Dependent Claims 3 and 16*

Claim 3 depends from claim 1 and further recites, “wherein said synchronized frame decryption stream includes encryption status information corresponding to each frame of said protected stream.” Ex. 1001, 11:64–67. Claim 16 depends from claim 14 and recites limitations similar to those recited in claim 3.

Petitioner contends that “[a] POSITA would [] have found it obvious to use Fetkovich’s density parameter to indicate an encryption status for each frame, where a density of 0 indicates the frame is unencrypted, and non-zero density values indicate the frame is partially encrypted.” Pet. 55 (citing Pet. §§ VI.A.1, VI.A.2[1d]; Ex. 1003 ¶¶ 132, 156, 196); *see id.* at 79–80 (addressing claim 16).

We are persuaded by Petitioner’s contentions, the cited portions of Fetkovich, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claims 3 and 16.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and

supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claims 3 and 16 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

8. *Dependent Claims 4 and 17*

Claim 4 depends from claim 1 and recites, “wherein said synchronized frame decryption stream includes a reference to a decryption key in the key table.” Ex. 1001, 12:1–3. Claim 17 depends from claim 14 and recites substantially similar features: “wherein said synchronized frame decryption stream includes a reference to a frame decryption key for each of said encrypted frames.” *Id.* at 13:6–8.

According to Petitioner, “Ueno’s teaching regarding key numbers includes references to both encryption keys and decryption keys in key tables, where the transmitter and receiver have the ‘same contents’ in their key tables, and the key numbers that are multiplexed into the data stream reference keys for decryption.” Pet. 56 (citing Ex. 1004, 1:32–57, 4:60–5:1, 5:33–44, 6:60–65; Ex. 1003 ¶ 200). Petitioner further contends that “[a] POSITA would have understood DES, Triple DES, Blowfish, FEAL, and AES to be symmetric encryption algorithms, meaning the same key is used for encryption and decryption” and “[t]hus the frame encryption key taught by the combination is obviously the same as the frame decryption key.” *Id.* (citing Ex. 1003 ¶¶ 199–200; *see id.* (citing Ex. 1004, 1:13–20 (teaching DES and FEAL algorithms)); Ex. 1006, 27:65–28:1; Ex. 1005, 6:52–56 (“Any conventional encryption technique can be employed within encryption unit 20 .....”); Pet. §§ IV, VI.A.1, n.3).

We are persuaded by Petitioner’s contentions, the cited portions of Ueno, Fetkovich, and Demos, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claims 4 and 17.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claims 4 and 17 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

9. *Dependent Claims 5, 6, 9, and 18*

Claim 5 depends from claim 1 and further recites “wherein said synchronized frame decryption stream includes intra-frame encryption offset information corresponding to each encrypted frame of said protected stream.” Ex. 1001, 12:4–7. Claim 18 depends from claim 14 and recites substantially similar limitations.

Petitioner contends that the “combination teaches partially encrypting portions of selected frames based on encryption parameters that are included as synchronized frame decryption information for each frame, which is part of the synchronized frame decryption stream.” Pet. 56–57 (citing Pet. §§ VI.A.2[1d–1g]; Ex. 1003 ¶ 202). Petitioner further contends that “[t]he encryption parameters include granularity, which selects the encryption unit such as a slice or macroblock, and delay, which ‘refers to the number of encryption units to wait before encrypting the first one’” and that the “delay and granularity parameters control the offset within each frame before encryption begins.” *Id.* at 57 (citing Ex. 1005, 5:29–59; Ex. 1003 ¶ 203).

We are persuaded by Petitioner’s contentions, the cited portions of Fetkovich, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claims 5 and 18.

Patent Owner contends that “*Fetkovich*’s ‘delay’ parameter, cited by Petitioner is not a per frame delay.” PO Resp. 60 (citing Ex. 1005, 5:59–60). More particularly, Patent Owner contends that “[a] delay of, for example, 1 in *Fetkovich* does not mean that encryption is delayed by one unit in each frame; it merely means encryption is delayed at the beginning of the overall encryption process.” *Id.* Therefore, according to Patent Owner, “*Fetkovich*’s ‘delay’ parameter is not a ‘per frame’ delay.” *Id.* (citing Ex. 2008 ¶ 145). Patent Owner also contends that, “even if Fetkovich’s delay was a per-frame delay, its ‘granularity’ dictating the amount of delay would not be a byte offset as required by the Claims” because “*Fetkovich*’s granularity is based on frame sub-structure, e.g., slice or frame or GOP.” *Id.* (citing Ex. 1005, 5:29–33; Pet. § II.B).

With respect to Patent Owner’s argument that “*Fetkovich*’s ‘delay’ parameter . . . is not a per frame delay” (*see* PO Resp. 60), Petitioner responds, and we agree, that “the combination relies on *Demos*’ teaching for frame-based encryption.” Pet. Reply 25. Petitioner contends, and we agree, that “combin[ing] *Demos*’ selection of frames with Fetkovich’s sub-frame encryption’ by selecting frames, as Demos teaches, and then applying Fetkovich’s encryption parameters with sub-frame granularity . . . results in a per-frame offset” and further, that “[t]he claims do not require a byte offset.” *Id.* at 26 (citing Ex. 1003 ¶ 131; Pet. Reply § I).

Claim 6 depends from claim 5 and further recites, “further including parsing said input stream in order to determine frame boundaries and frame

types associated with frames of said sequence of frames.” Ex. 1001, 12:8–11.

Petitioner contends that “Demos teaches selecting frames for partial encryption based on frame type, particularly I and P frames.” Pet. 58 (citing Pet. §§ VI.A.1, VI.A.2[1d]). Petitioner further contends that “it would have been obvious to parse the input stream to determine frame boundaries and frame types (e.g., I, P, or B-frames) associated with frames of said sequence of frames.” *Id.* (citing Ex. 1006, 22:63–23:8; Ex. 1003 ¶ 206).

We are persuaded by Petitioner’s contentions, the cited portions of Demos, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claim 6.

Claim 9 depends from claim 6 and further recites “maintaining counts corresponding to each of said frame types, said counts being used to determine when to use a new frame encryption key in said encrypting of said selected frames.” Ex. 1001, 12:20–23.

According to Petitioner, “Fetkovich teaches updating keys based on a count of frames, with an example where the key is updated every 16 frames.” Pet. 59 (citing Ex. 1005, 6:24–40 (referring to frames as pictures); Ex. 1003 ¶¶ 208–214). Petitioner contends that “Fetkovich teaches two parameters for updating keys,” including “[t]he ‘Key Update Unit’ [which] ‘refers to the unit which is to be *tabulated* in order to determine when the encryption key is to be updated. This unit might be one of the granularities described above (picture, slice, etc.).” *Id.* (citing Ex. 1005, 5:62–6:2). Petitioner explains that “[t]he key update frequency ‘refers to the data interval at which the key is to be refreshed.” *Id.* (citing Ex. 1005, 6:3–6, 6:24–40).

Petitioner also contends that “Fetkovich further teaches that ‘[v]arying of the encryption parameter(s) is preferably responsive to data content’ explaining that ‘one trigger might be the passage of a certain number of units, where units are specific to the format in which the data is stored.’” *Id.* (citing Ex. 1005, 8:30–33). “When combined with Demos, a POSITA would have found it obvious to allow the Key Update Unit to specify not just a frame (picture), but also the type of frame, which is specific to the format in which the video stream is stored.” *Id.* at 60 (citing Ex. 1003 ¶ 211). As “Demos teaches the security impact of encrypting different types of frames, including I, P, and B frames,” it “teaches that the type of frame should be considered when partially encrypting video, and a POSITA would have been motivated, based on this teaching, to include the frame type (‘I-frame,’ ‘P-frame,’ or ‘B-frame’) for Fetkovich’s Key Update Unit.” *Id.* (citing Ex. 1006, 24:46–49, 23:2–7; Ex. 1003 ¶ 211).

We are persuaded by Petitioner’s contentions, the cited portions of Demos, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitation recited in claim 9.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b) for dependent claims 5, 6, 9, and 18, which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claims 5, 6, 9, and 18 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

*10. Dependent Claims 10 and 19*

Claim 10 depends from claim 1 and further recites “wherein said synchronized frame decryption stream includes information identifying a data field size to be decrypted with respect to each encrypted frame of said protected stream.” Ex. 1001, 12:24–26. Claim 19 depends from claim 14 and recites limitations substantially similar to claim 10.

Petitioner contends that “[t]he synchronized frame decryption stream includes synchronized frame decryption information, including partial encryption parameters, with respect to each encrypted frame of said protected stream.” Pet. 62–63 (citing Pet. §§ VI.A.2[1d–1g]; Ex. 1003 ¶ 216). Petitioner explains that “[t]he encryption parameters include granularity, which selects the size of the encryption unit, such as a slice or macroblock” and “Fetkovich provides an example where granularity is a slice and every fourth slice is encrypted, meaning the data field size of each encrypted portion is 1 slice.” *Id.* at 63 (citing Ex. 1005, 5:28–60; 6:24–40; Ex. 1003 ¶ 217). Petitioner further contends that “Fetkovich explains that ‘[d]ecryption of the stream is then performed on the receiving end’ ‘which then decrypts the data using the encryption information’” and that Fetkovich’s “encryption parameters, including granularity, are used to decrypt the encrypted MPEG video stream.” *Id.* (citing Ex. 1005, 2:11–12, 6:66–7:7, Fig. 1; Ex. 1003 ¶ 218). According to Petitioner, “[t]hus the granularity parameter controls a data field size that is encrypted in each frame, and identifies a data field size to be decrypted with respect to each partially encrypted frame of said protected stream.” *Id.* (citing Ex. 1003 ¶ 219).

Patent Owner contends that “[i]t is undisputed that *Fetkovich*’s ‘granularity’ encryption parameter identifies portions of the frame to be decrypted (or encrypted) based on frame sub-structure,” and that, “[f]or example, the unit of encryption may be a slice.” PO Resp. 61 (citing Ex. 1005, 5:29–33). Patent Owner further contends that “in a compressed stream, frame substructures such as slices do not have a pre-determined or fixed ‘size.’” *Id.* Thus, according to Patent Owner, although “*Fetkovich*’s system may specify that every fourth slice is encrypted,” it “cannot specify or convey the ‘data field size’ of encryption, because the size of each slice widely varies depending on how much compression may be achieved.” *Id.* at 61–62 (citing Ex. 2008 ¶ 150).

Like Petitioner, we characterize Patent Owner’s arguments as ones that contend “data field size cannot be based on slices or macroblocks” even though “slices and macroblocks are common ‘units’ of video data.” Pet. Reply 26 (citing Pet. Reply § I.C). Petitioner contends, and we agree, that “[t]he ’673 patent expressly allows the data field size to be expressed in terms of data ‘units,’ for which a byte is just one example” and as such, “the ’673 patent allows the data field size to be expressed in terms of slices and macroblocks.” *Id.* (citing Ex. 1001, 6:25–38); *supra* § II.A. Accordingly, we find Patent Owner’s arguments to be unavailing.

We are persuaded by Petitioner’s contentions, the cited portions of *Fetkovich*, and Dr. McDaniel’s testimony that the combination of Ueno, *Fetkovich*, and Demos teaches the limitations recited in claims 10 and 19. Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in

Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claims 10 and 19 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

*11. Dependent Claim 13*

Claim 13 depends from claim 1 and further recites

further comprising: receiving an input stream of video content containing a sequence of frames; and generating the input stream of compressed video content by applying processing techniques in accordance with an applicable encoding standard to produce a plurality of video information streams; wherein the encrypting of selected frames includes encrypting a portion of a predetermined video information stream.

Ex. 1001, 12:37–46.

Petitioner contends that “Demos teaches receiving an input stream of video content (e.g., captured or uncompressed video) containing a sequence of frames.” Pet. 64 (citing Ex. 1006, 2:58–60 (“Image material is preferably captured at an initial or primary framing rate of 72fps. An MPEG-2 data stream is then generated . . .”), 8:15–9:18 (“MPEG-2 . . . provides an efficient way to represent image sequences.....”); Ex. 1003 ¶ 224).

Petitioner contends that “Demos teaches compressing the input stream . . . using MPEG-2 to generate the input stream of *compressed* MPEG video content (referenced in claim 1), by applying processing techniques in accordance with the applicable MPEG-2 encoding standard.” *Id.* at 65–66 (citing Ex. 1006, 2:58–60, 8:40–56; Ex. 1003 ¶ 226). Petitioner further contends that Demos “teaches that the generated input stream of compressed video content includes a plurality of MPEG-2 video information streams (e.g., DC coefficients, AC coefficients, motion vectors),” as well as “collecting and aggregating DC coefficients, AC coefficients, and motion

vectors from MPEG-2 video.” *Id.* at 66 (citing Ex. 1006, 23:37–67, 24:20–40; Ex. 1003 ¶ 227). Petitioner also contends that Fetkovich “teaches the use of MPEG video, explaining additional components of the video information streams, including macroblocks and slices,” and that, thus, “for the combined teachings of the references, a POSITA would have understood DC coefficients, AC coefficients, macroblocks, and slices to be part of the plurality of video information streams produced by applying processing techniques in accordance with an applicable MPEG encoding standard.” *Id.* (citing Ex. 1003 ¶¶ 229–231; Ex. 1005, 3:4–14, 5:31–33; Ex. 1006, 23:58–24:15; Ex. 1001, 10:39–43, 10:47–49).

Petitioner further contends that the “combination renders obvious encrypting DC or AC coefficients of selected frames,” which “would each be a portion of a predetermined video information stream, such as the video information stream comprising quantized DCT coefficients.” *Id.* at 67 (citing Ex. 1003 ¶ 232; Pet. § VI.A.2[1d]). Petitioner contends that, alternatively, “the combination also renders obvious encrypting selected macroblocks and slices from selected frames, e.g., every other minute or important scenes.” *Id.* (citing Pet. § VI.A.2[1d]). Petitioner further contends that “[t]his would have included encrypting a portion of a predetermined video information stream (e.g., selected macroblocks or slices).” *Id.* (citing Ex. 1003 ¶ 233).

We are persuaded by Petitioner’s contentions, the cited portions of Fetkovich and Demos, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claim 13.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and

supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes unpatentability of claim 13 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

*12. Dependent Claim 15*

Claim 15 depends from claim 14 and further recites “wherein said input stream and said synchronized frame decryption stream collectively comprise a protected video stream, said synchronized frame decryption stream being synchronized with said encrypted frames within said input stream.” Ex. 1001, 12:65–13:2.

According to Petitioner, “[t]he combination teaches or suggests receiving as input the protected video stream from claim 1, which includes an input stream of compressed video content and the synchronized frame decryption stream,” and that, “[i]n the protected stream, the frame decryption information is synchronized with the set of encrypted frames into a synchronized frame decryption stream.” Pet. 79 (citing Ex. 1003 ¶¶ 258–259; Pet. §§ VI.A.2[1b, 1e–1g], Pet. §§ VI.A.11[14a–14d]).

We are persuaded by Petitioner’s contentions, the analysis and underlying cited disclosures in Section VI of the Petition, and Dr. McDaniel’s testimony that the combination of Ueno, Fetkovich, and Demos teaches the limitations recited in claim 15.

Petitioner relies on the same motivation to combine as set forth for independent claim 1 (*supra* § III.A.4.b), which we find persuasive and supported by sufficient rational underpinnings for the reasons set forth in Section III.A.4.c. Accordingly, we are persuaded that Petitioner establishes

unpatentability of claim 15 over the combination of Ueno, Fetkovich, and Demos by a preponderance of the evidence.

*B. Petitioner's Motion to Exclude and Motion to Strike*

Petitioner timely objected to Patent Owner's evidence (Papers 23, 24, 51) and thereafter filed a Motion to Exclude Exhibits 2004–2007, 2010–2020, and 2032. Mot. Ex. Patent Owner opposed Petitioner's Motion to Exclude (Paper 53), and Petitioner replied to Patent Owner's Opposition (Paper 58). Petitioner also filed a Motion to Strike Exhibit 2032 and portions of Patent Owner's Sur-Reply (Paper 55), Patent Owner opposed (Paper 61), and Petitioner replied to Patent Owner's Opposition (Paper 64).

*1. Exhibits 2004–2006, 2010, and 2020*

In its Motion to Exclude, Petitioner requests exclusion of Exhibits 2004, 2005, 2006, 2010, and 2020 for not being authenticated (Fed. R. Evid. 901(a)), containing inadmissible hearsay (Fed. R. Evid. 801(c), 802; 37 C.F.R. § 42.53), improper opinions (Fed. R. Evid. 701, 602), and lacking relevance (Fed. R. Evid. 402). Mot. Ex. 6–10. Petitioner's Motion to Exclude is dismissed as moot with respect to Exhibit 2020 because our decision would not be affected by the admission or exclusion of that exhibit—we do not rely on it in reaching our conclusion as to the patentability of the challenged claims.

We are not persuaded by Petitioner's arguments and do not agree that Exhibits 2004–2006 and 2010 are not authenticated, contain inadmissible hearsay and improper opinions, and lack relevance. Mot. Ex. 6–10. Instead, we find persuasive Patent Owner's arguments as to the admissibility of these exhibits. PO Opp. Ex. 5–9. We consider Exhibits 2004–2006 and 2010 for the limited purpose of evaluating nexus with respect to Patent Owner's

evidence of objective indicia of nonobviousness—which we determine is not shown (*supra* § III.A.4.e)—and afford these exhibits the appropriate weight.

As the factfinders, we are able to consider the evidence offered by Petitioner and Patent Owner, in light of the parties’ arguments, and give it the appropriate weight, without risk of unfair prejudice. *See* Wright & Miller, 22A Fed. Prac. & Proc. Evid. § 5213 (2d ed.) (“In bench trials . . . appellate courts have said that exclusion of evidence on grounds of ‘prejudice’ makes little sense because the judge has to see the putatively prejudicial evidence in order to rule.”); *see also* *Schultz v. Butcher*, 24 F.3d 626, 632 (4th Cir. 1994) (courts should not exclude evidence under Rule 403 in non-jury trial on grounds of unfair prejudice).

## 2. *Exhibits 2007 and 2011–2019*

Petitioner requests exclusion of Exhibits 2007 and 2011–2019 for lack of authentication (Fed. R. Evid. 901(a)), containing inadmissible hearsay (Fed. R. Evid. 801(c), 802; 37 C.F.R. § 42.53), and containing improper opinions (Fed. R. Evid. 701, 602). Mot. Ex. 10–13. We dismiss as moot Petitioner’s Motion to Exclude with respect to Exhibits 2007, 2011, 2012, 2014–2016, 2018, and 2019, because we do not rely on any of these exhibits—which mostly constitute general background knowledge of encryption—in rendering our findings and conclusions in this Decision. We also note that Exhibits 2012–2014, 2016, and 2018 were published after the earliest possible priority date (October 23, 2002), and after the later filing date (July 8, 2003), of the ’673 patent. And Exhibits 2012, 2013, 2016, and 2018 were published after the issuance of the ’673 patent (November 13, 2007).

With respect to Exhibit 2017, which is “An Empirical Study of Secure MPEG Transmission,” we deny Petitioner’s Motion to Exclude. We are not persuaded by Petitioner’s arguments and do not agree that Exhibit 2017 is not authenticated and contains inadmissible hearsay as well as improper opinions. Mot. Ex. 10–13. Instead, we find persuasive Patent Owner’s arguments for the admissibility of this exhibit. PO Opp. Ex. 9–15. We consider Exhibit 2017 for the limited purpose of evaluating nexus with respect to Patent Owner’s evidence of objective indicia of nonobviousness—which we determine is not shown (*supra* § III.A.4.e)—and afford this exhibit the appropriate weight, without the risk of unfair prejudice.

3. *Exhibit 2032 and Portions of Patent Owner’s Sur-Reply*

Petitioner also requests exclusion of Exhibit 2032, an article titled “Why the DVD Hack Was a Cinch,” by Andy Patrizio on Wired.com, as being impermissible new Sur-Reply evidence, as well as for being irrelevant (37 C.F.R. § 42.23(b); Fed. R. Evid. 402), not authenticated (Fed. R. Evid. 901(a)), and containing inadmissible hearsay (Fed. R. Evid. 801(c), 802). Mot. Ex. 2–6.

Exhibit 2032 is also the subject of Petitioner’s Motion to Strike. In addition to Exhibit 2032, Petitioner requests that we strike Patent Owner’s “Sur-Reply [a]rguments [a]ttacking the [u]se of Ueno’s [k]ey [n]umbers to [f]acilitate Demos’ [f]rame [s]election.” Mot. St. 3 (emphasis omitted). Petitioner contends that arguments on pages 20 to 21 of Patent Owner’s Sur-Reply constitute “unsupported, erroneous attorney argument regarding, for example, the number of bits required to identify an encrypted frame and the number of bits required for sending the key number with each frame, as well as counsel’s opinions on whether something takes ‘more data’ and whether

there is ‘apparent benefit.’” *Id.* at 4. Petitioner further argues that Patent Owner did not address the explanation in the Petition that, “by sending a key number with each frame, the key number can indicate the encryption key for that frame (if the frame is encrypted) or that no encryption key was used (if the frame is not encrypted).” *Id.* (citing Pet. 51, 54; Ex. 1003 ¶¶ 188, 195).

We dismiss Petitioner’s Motion to Exclude as to Exhibit 2032 as moot. Similarly, we dismiss Petitioner’s Motion to Strike Exhibit 2032 and portions of Patent Owner’s Sur-Reply on pages 24 and 25 as moot. This is because Patent Owner’s arguments concerning Exhibit 2032 are about transmitting an encryption key *with each frame* to “improve security.” PO Sur-Reply 23. As discussed above in Section II.B, we do not construe “synchronized frame decryption stream” to require sending frame decryption information in a 1:1 correspondence with encrypted frames. As such, we do not consider, and need not exclude or strike, Exhibit 2032 and Patent Owner’s Sur-Reply arguments that implicitly construe “synchronized frame decryption stream” in a manner which we did not adopt.

*C. Petitioner and Patent Owner’s Objections to Demonstratives*

Petitioner objects to portions of Patent Owner’s oral hearing demonstratives. Paper 65. Patent Owner objects to portions of Petitioner’s oral hearing demonstratives. Paper 66. As the demonstratives are not evidence, and because our Decision does not reference the demonstratives, we need not and do not address the parties’ objections beyond dismissing both parties’ objections as moot.

*D. Patent Owner’s Motion to Seal and Motion for Protective Order*

In its Motion to Seal, Patent Owner argues that Exhibits 2004–2006, 2010, and 2020 should be sealed. *See generally* Mot. Seal. Patent Owner also

argues for us to grant its Unopposed Motion for Entry of Protective Order.  
Mot. Prot.

According to Patent Owner, “Exhibit 2004 is a closely held document that describes highly confidential descriptions of products of Patent Owner DivX, LLC . . . including information relating to security measures which Patent Owner keeps confidential for trade secret and competitive reasons.” Mot. Seal 2. Patent Owner notes that Exhibit 2004 “is designated as HIGHLY CONFIDENTIAL PROTECTIVE ORDER MATERIAL.” *Id.* at 3. Patent Owner contends that Exhibit 2005 has the same designation and is also “a closely held document that describes highly confidential descriptions of DivX products including information relating to security measures which Patent Owner keeps confidential for trade secret and competitive reasons.” *Id.* Patent Owner further contends that “Exhibit 2006 is a document marked and created as confidential directed at potential investors, using confidential information obtained from DivX, describing aspects of DivX’s business and products” and “contain[ing] business confidential information concerning profitability and projected growth” and is “designated as PROTECTIVE ORDER MATERIAL.” *Id.* at 3–4. Patent Owner further contends that “Exhibit 2010 is a closely held document that describes highly confidential descriptions of DivX products including information relating to security measures which Patent Owner keeps confidential for trade secret and competitive reasons” and “is designated as HIGHLY CONFIDENTIAL PROTECTIVE ORDER MATERIAL.” *Id.* at 4. Patent Owner finally contends that “Exhibit 2020 is a claim chart which references, cites, or otherwise utilizes confidential information contained in Exhibit 2010 (which is designated as HIGHLY

CONFIDENTIAL PROTECTIVE ORDER MATERIAL” and “for the same reasons . . . that . . . Exhibit 2010 is . . . designated as described above, Exhibit 2020 is [also] designated as HIGHLY CONFIDENTIAL PROTECTIVE ORDER MATERIAL.” *Id.*

Petitioner contends that Patent Owner does not show good cause for sealing the Exhibits discussed above because Patent Owner does not identify the specific information it believed to be confidential, does not explain what harm would result from public disclosure of the information, does not explain a genuine need to rely in the trial on the specific information sought to be sealed, and does not show an interest in maintaining confidentiality outweighs the strong public interest in having an open record. Pet. Opp. Mot. Seal 5, 9, 11, 12. Petitioner further contends that designating the exhibits (as confidential) in the District Court does not bind the Board’s Decision in this case. *Id.* at 13.

We are not persuaded by Petitioner’s arguments and are, instead, persuaded by Patent Owner’s contentions that the Board routinely seals information relating to a party’s products and financial information and that the balance of factors favors the limited sealing request. PO Reply Mot. Seal 2, 4; *see also* Mot. Seal (Patent Owner arguing reasons to seal Exhibits 2004–2006, 2010, and 2020). As such, we grant Patent Owner’s Motion to Seal in its entirety and also grant Patent Owner’s Motion for Entry of Protective Order. Mot. Seal; Mot. Prot.

#### IV. PATENT OWNER’S CONSTITUTIONALITY ARGUMENTS

Patent Owner contends that “[t]he Board’s organization, including its incentive and fee structure, violates the due process and Administrative Procedure Act right to an impartial, disinterested tribunal, *see, e.g., Ward v.*

*Vill. Of Monroeville*, 409 U.S. 57 (1972), by improperly encouraging decisions in favor of institution, including this one.” PO Resp. 62.

Patent Owner contends that “[t]he PTAB business unit keeps more (*i.e.*, pre-paid post-institution) IPR fees (which fund nearly half its AI[A] trial budget), and the assigned Board panel grants itself more work and greater opportunity for work ‘production’ and performance review credits, each time the panel grants rather than denies institution on the Director’s behalf.”

*Id.* According to Patent Owner,

[t]he Board thus enjoys both pecuniary and employment benefits from granting institution. The line APJs’ lack of Title 5 job protections and independence under *Arthrex, Inc. v. Smith & Nephew, Inc.*, 941 F.3d 1320 (Fed. Cir. 2019), *reh’g denied*, 953 F.3d 760 (Fed. Cir. 2020) (en banc), *cert. granted*, *Smith & Nephew, Inc. v. Arthrex, Inc.*, 2020 U.S. Lexis 4928 (S. Ct. Oct. 13, 2020), and the Lead ALJs’ mixture of administrative and adjudicative functions, add the further appearance of bias. Although the Board has declined to adjudicate its procedures’ constitutionality, *e.g.*, *ZTE (USA) v. Fundamental Innovation Sys. Int’l*, IPR2018-00425, Paper 52, 29 (PTAB Jul. 2, 2019), and cannot change, waive or cure the organizational features described above, the appropriate remedy is dismissal.

*Id.* at 62–63.

Patent Owner further contends that “the Board is unconstitutionally appointed to decide IPRs” and that “[e]liminating Board tenure protections cannot cure that problem.” *Id.* at 63 (citing *Arthrex, pet. for cert. filed*, 19-1458 (June 30, 2020)). Patent Owner takes the position that, “[e]ven if a cure were possible without Congressional confirmation or higher agency review, it cannot be done by ‘retroactively’ ‘severing’ long-guarded protections in a long-standing, different statute.” *Id.*

Additionally, Patent Owner contends that, “[b]ecause Patent Owner is not before the Board by choice, and no properly-appointed Board panel is available, the appropriate remedy is not severance, but dismissal.” *Id.*

Patent Owner raises two Constitutional arguments relating to the Board’s ability to render a decision in this proceeding including: (1) that the Board’s organization, including its incentive and fee structure, violates due process and the right to an impartial, disinterested tribunal; and (2) that the Board was unconstitutionally appointed. *Id.* at 62–63. We decline to address Patent Owner’s constitutional challenge except to note that the constitutionality of the appointments of the Administrative Patent Judges was addressed by the U.S. Supreme Court in *United States v. Arthrex, Inc.*, 141 S. Ct. 1970, 1986–87, 1997 (2021).

## V. CONCLUSION

For the foregoing reasons, we conclude that Petitioner has established unpatentability of claims 1–6, 9, 10, and 13–19 by a preponderance of the evidence.<sup>8</sup> Our conclusion regarding the challenged claims is also presented below:

---

<sup>8</sup> Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. §§ 42.8(a)(3), (b)(2).

| <b>Claim(s)<br/>Challenged</b> | <b>35<br/>U.S.C. §</b> | <b>Reference(s)/Basis</b> | <b>Claims Shown<br/>Unpatentable</b> | <b>Claims Not<br/>Shown<br/>Unpatentable</b> |
|--------------------------------|------------------------|---------------------------|--------------------------------------|----------------------------------------------|
| 1–6, 9, 10,<br>13–19           | 103                    | Fetkovich, Demos,<br>Ueno | 1–6, 9, 10, 13–<br>19                |                                              |

## VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–6, 9, 10, and 13–19 of the '673 patent are determined to be unpatentable;

FURTHER ORDERED that Petitioner's Motion to Exclude is dismissed as moot with respect to Exhibits 2020, 2007, 2011–2016, 2018, and 2032, and denied with respect to Exhibits 2004–2006, 2010, and 2017;

FURTHER ORDERED that Petitioner's Motion to Strike is dismissed as moot;

FURTHER ORDERED that Patent Owner's Motion for Entry of Protective Order is granted;

FURTHER ORDERED that Patent Owner's Motion to Seal is granted in its entirety and Exhibits 2004-2006, 2010, and 2020 and this Decision are to be sealed;

FURTHER ORDERED that the parties shall jointly submit to the Board a proposed redacted version of the Final Written Decision (Paper 68) within 14 days of this Decision;

FURTHER ORDERED that Patent Owner's and Petitioner's Objections to Demonstratives are each dismissed as moot; and

FURTHER ORDERED that, because this a Final Written Decision, parties to this proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2020-00614  
Patent 7,295,673 B2

For PETITIONER:

Harper Batts  
Chris Ponder  
Jeffrey Liang  
SHEPPARD, MULLIN, RICHTER & HAMPTON, LLP  
hbatts@sheppardmullin.com  
cponder@sheppardmullin.com  
jliang@sheppardmullin.com

For PATENT OWNER:

Kenneth Weatherwax  
Nathan Lowenstein  
Bridget Smith  
Flavio Rose  
Edward Hsieh  
Parham Hendifar  
Patrick Maloney  
LOWENSTEIN & WEATHERWAX LLP  
weatherwax@lowensteinweatherwax.com  
lowenstein@lowensteinweatherwax.com  
smith@lowensteinweatherwax.com  
rose@lowensteinweatherwax.com  
hsieh@lowensteinweatherwax.com  
hendifar@lowensteinweatherwax.com  
maloney@lowensteinweatherwax.com