Trials@uspto.gov
571-272-7822

Paper 30
Entered: March 6, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2022-01587
Patent 10,237,282 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and CHRISTOPHER L. OGDEN, *Administrative Patent Judges.*

CALVE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Netskope, Inc. ("Petitioner") filed a petition requesting *inter partes* review of claims 1–8 and 11–18 (the "challenged claims") of U.S. Patent No. 10,237,282 B2 ("the '282 patent") (Ex. 1001). Paper 2 ("Pet."), 1. Fortinet, Inc. ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp."). Applying the standard in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims on all grounds asserted in the Petition. Paper 9 ("Dec. Inst.").

After we instituted trial, Patent Owner filed a Patent Owner Response. Paper 16 ("PO Resp."). Petitioner filed a Reply to Patent Owner's Response. Paper 20 ("Reply"). Patent Owner filed a Sur-reply to Petitioner's Reply. Paper 26 ("Sur-reply").

An oral hearing was held on February 1, 2024, and a copy of the transcript was entered in the record. Paper 29.

We have jurisdiction pursuant to 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) (2018) and 37 C.F.R. § 42.73 (2020) as to the patentability of the claims on which we instituted trial. Petitioner bears the burden of proving unpatentability of the challenged claims. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–8 and 11–18 of the '282 patent are unpatentable.

II. BACKGROUND

A. Related Proceedings

The parties identify the following proceeding in which the '282 patent is involved: *Netskope, Inc. v. Fortinet, Inc.*, Case No. 3:22-cv-01852-JSC (N.D. Cal.). Pet. 1; Paper 4 (Patent Owner's Mandatory Notices), 2.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the sole real party in interest. Pet. 1. Patent Owner identifies Fortinet, Inc. as the sole real party in interest. Paper 4, 2.

C. The '282 Patent

The '282 patent describes techniques for Data Leak Prevention (DLP) in enterprise networks. Ex. 1001, 1:62–63, 3:6–7. The '282 patent issued after Patent Owner filed a terminal disclaimer to overcome a nonstatutory double patenting rejection. Ex. 1010, 97–98, 134, 142.

Digital watermarks may be used as a security measure to prevent data leaks. Digital watermark technology embeds information in data such as an image, document, and voice. Ex. 1001, 1:50–54. A "watermark" includes:

> information or a fingerprint embedded within a document that is indicative of one or more of a source, origin, owner or author of the document (e.g., a company, group, division, end user or other entity or person) and a sensitivity level of the document or information contained therein (e.g., critical, high, medium, low). According to one embodiment, a watermark includes plain text (a visible watermark) or encoded information (an invisible watermark) containing a company identifier and a sensitivity level. In other embodiments, the watermark is a value (e.g., a hash value) that can be used to look up the associated company identifier and sensitivity level.

Id. at 4:64–5:9.

A DLP sensor may be configured at gateway 104, which interfaces network 100a with network 100b of an intra company network and controls network transmissions between computer systems 106a–d and Internet 102, as shown in Figure 1, reproduced below. Ex. 1001, 5:10–45, 6:40–50.

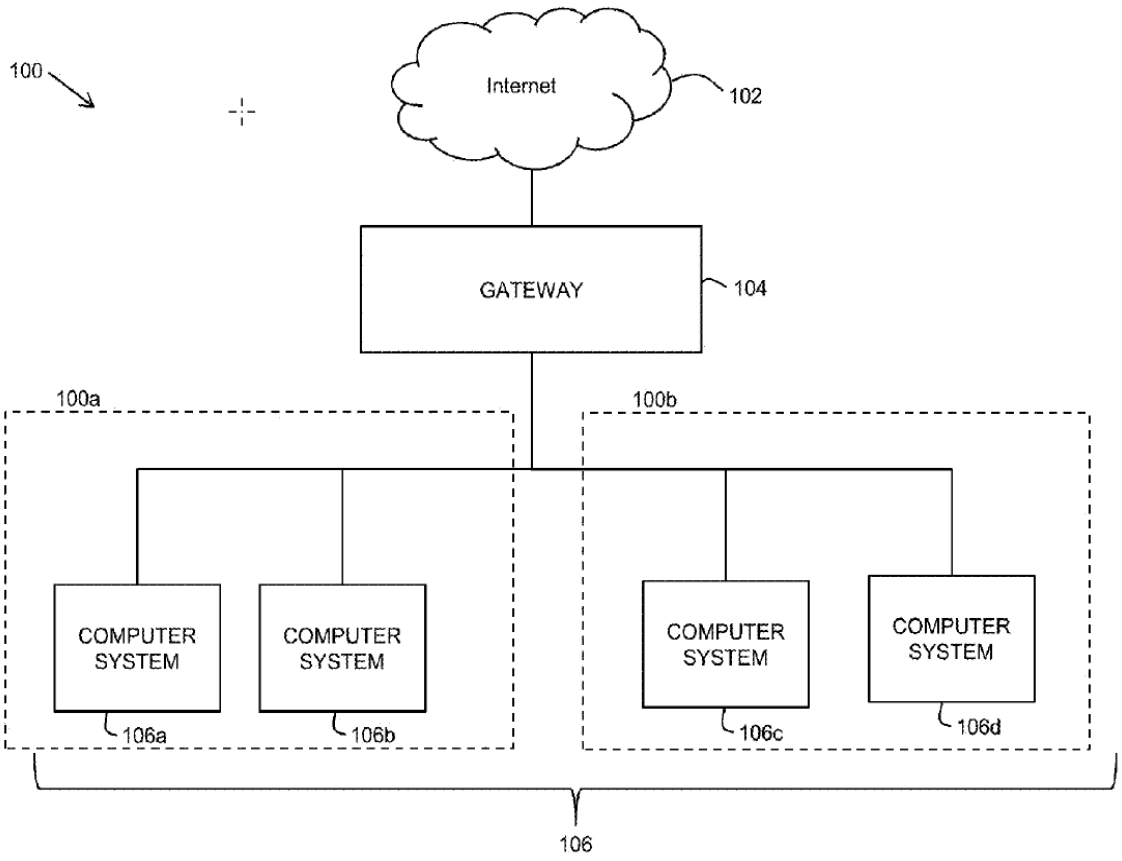


FIG. 1

Figure 1 depicts network 100 including Internet 102, gateway 104, and computer systems 106a–d. Ex. 1001, 5:10–19. Gateway 104 interfaces networks 100a and 100b and acts as a proxy server and/or firewall server that protects the networks from unauthorized access while permitting legitimate communication to pass based on a set of rules. *Id.* at 5:26–45.

To provide DLP for network 100, users may configure a DLP sensor at gateway 104 to detect watermarks in files, extract payloads contained in the watermarks, and block or pass files at gateway 104 according to filtering rules described below. Ex. 1001, 6:40–50. Figure 2 of the '282 patent is reproduced below to illustrate the functional units of gateway 104.

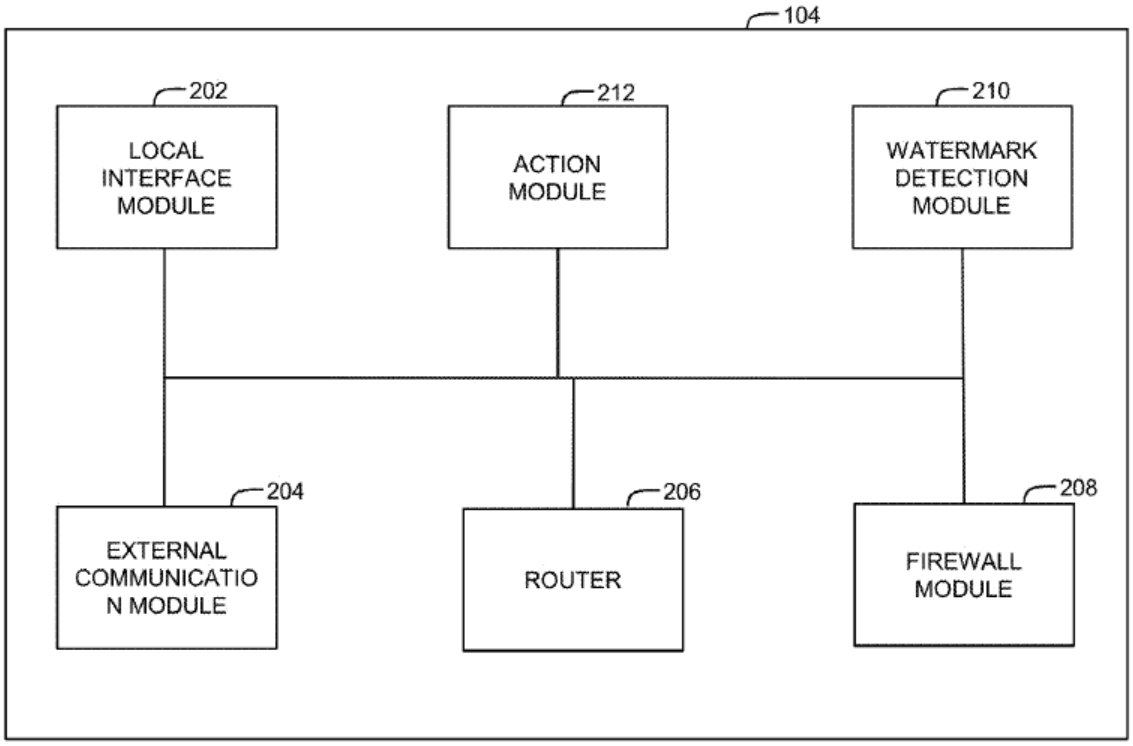


FIG. 2

Figure 2 is a block diagram illustrating the functional units of gateway 104. *Id.* at 6:64–66. Local interface module 202 provides a physical and data-link layer communication interface with computer systems 106a–d. External interface module 204 accepts/provides IP packets over data paths to/from the other modules of gateway 104. Router 206 routes data packets along data paths in gateway 104 and is connected to firewall module 208 that permits or denies network transmissions based on a set of rules. *Id.* at 7:4–25.

Watermark detection module 210 includes a package of DLP rules. Traffic passing through gateway 104 is searched for patterns defined by the DLP rules. Ex. 1001, 7:39–43. If matching traffic is found, action module 212 takes action on the file as specified in the DLP rules such as blocking the file at gateway 104, allowing the file to pass through gateway 104, or logging the traffic. *Id.* at 7:43–47. The modules are a suitable type of logic. *Id.* at 7:48–62. Figure 10 of the '282 patent, reproduced below, as redrawn by Petitioner for clarity (Pet. 34), illustrates a graphical user interface (GUI) that is used to create a new DLP sensor filter. *Id.* at 7:42–43 (indicating that DLP rules are described with reference to Figures 9 and 10).

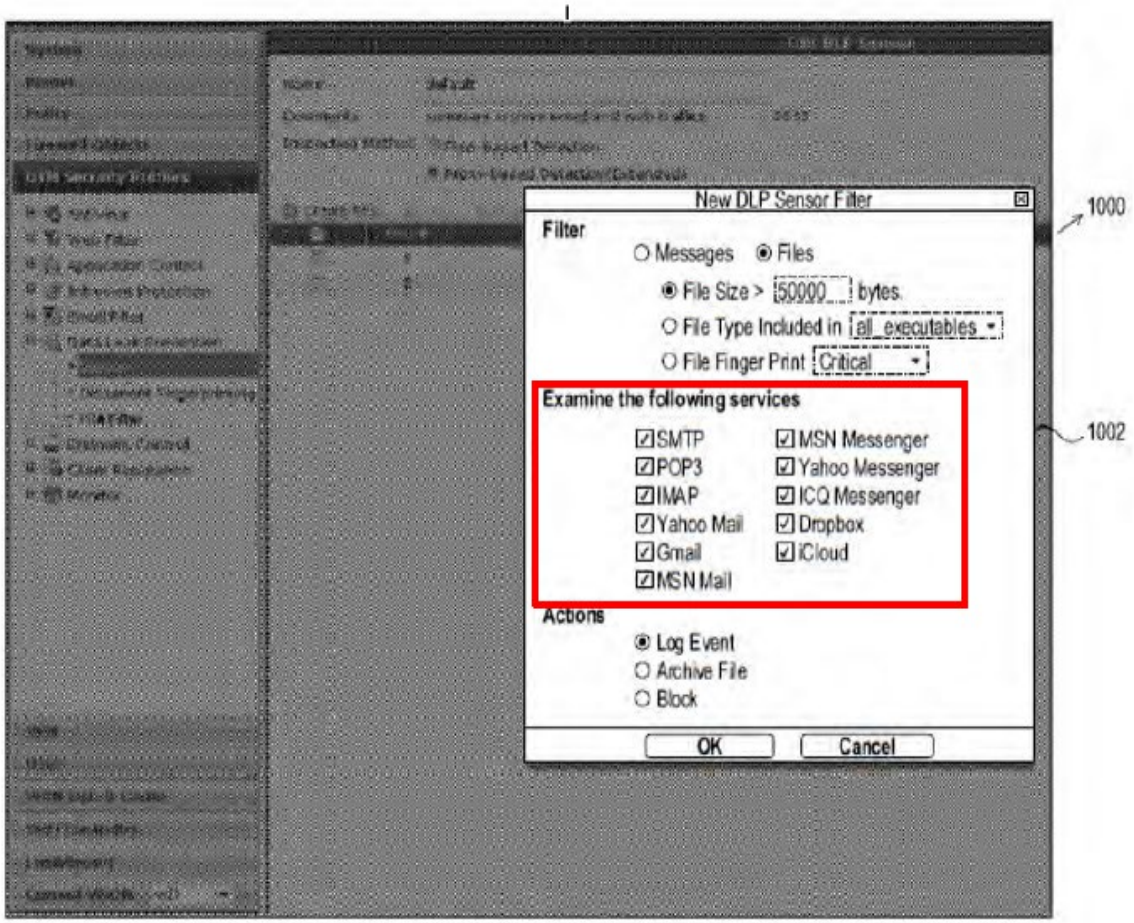


FIG. 10 (Redrawn)

Figure 10 shows GUI 1000 used to create a New DLP Sensor Filter for files communicated over enterprise network 100. *Id.* at 13:22–24. To define a rule for files, the user selects "Files" in dialog box 1002. *Id.* at 13:24–25. Dialog box 1002 has sub-fields for "Files" to include "File size," "File type Included in," and "File fingerprint." *Id.* at 13:26–28. In the example of Figure 10, because a user selected a file size greater than or equal to 50,000 bytes, the DLP sensor filters and examines any file size that is greater than or equal to 50,000 bytes. The "File Type included in" drop down menu allows selection of "all_executables" and "all_archives." *Id.* at 13:29–40.

A user may create a filter for a watermark detected in a file using the drop-down menu "File Fingerprint" to specify a watermark's sensitivity as critical, high, medium, or low sensitivity, and to specify an action to take when a watermark matches the DLP filter such as log event, archive message, or block message. Ex. 1001, 13:11–13, 13:41–62, 14:30–34.

A user may create individual filters for "Files" or combine filters that define file size, type, and watermark/fingerprint. A user may select network services to examine for DLP filter criteria and define an action to take for a match. Ex. 1001, 13:48–54. Network services can include SMTP, POP3, IMAP, Yahoo Mail, Gmail, MSN Mail, MSN Messenger, and Yahoo Messenger. *Id.* at 13:8–11. Thus, for a filter defined for a file size of at least 50,000 bytes with a file fingerprint of *Critical* and Action of *Block*, gateway 104 monitors the selected services to detect files of Critical sensitivity level and relevant size (e.g., 60,000 bytes) and blocks those files at gateway 104 from reaching their intended destination. *Id.* at 13:55–62.

Figure 11 is reproduced below to depict a DLP process performed at a filtering device such as gateway 104. Ex. 1001, 13:63–14:34.

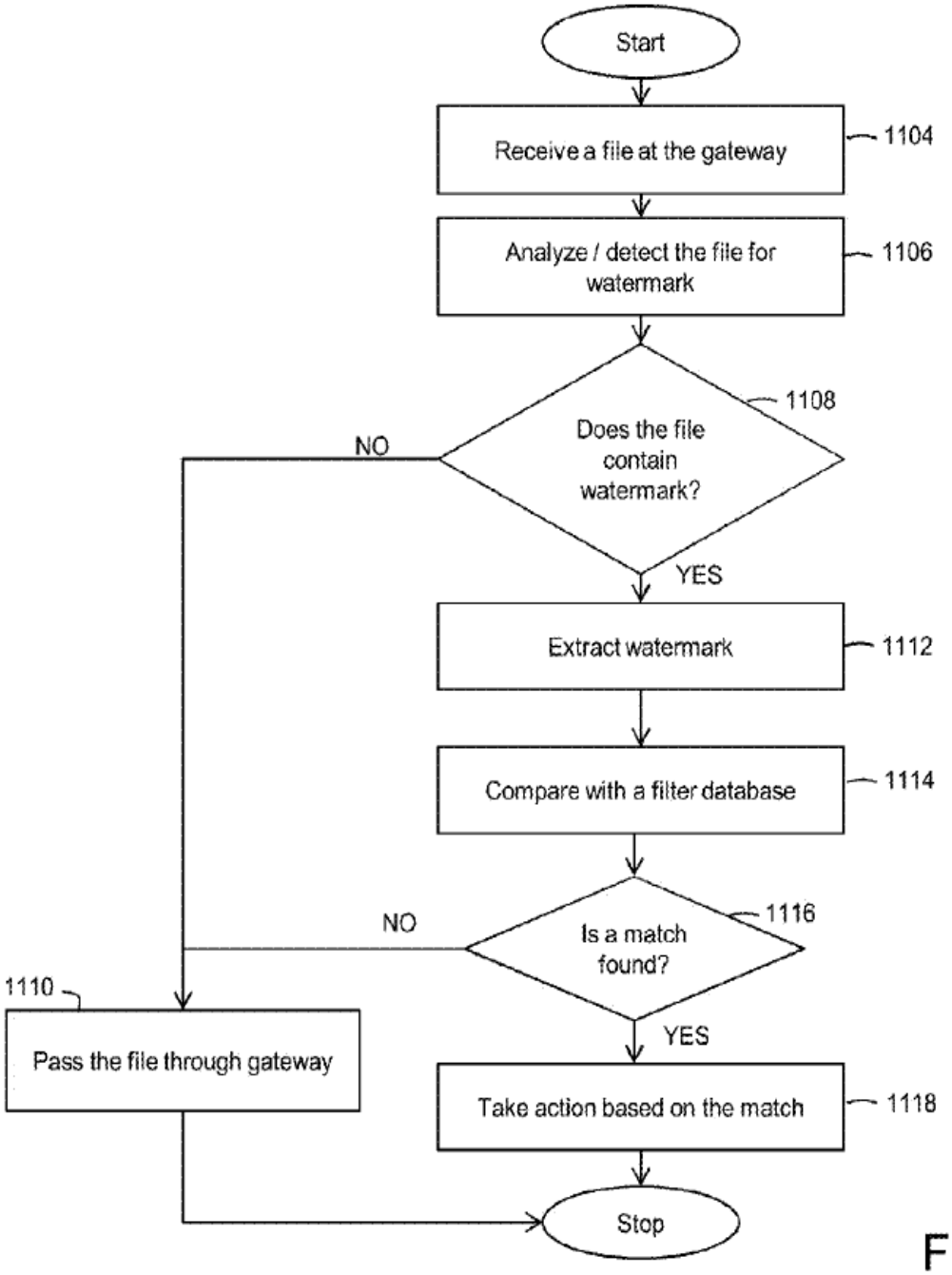


FIG. 11

Figure 11 is a flow diagram for receiving a file at gateway 104 (step 1104), detecting and extracting a watermark (steps 1106–1112), comparing the watermark to rules in a database (step 1114), and taking action of blocking or allowing a file to pass if a match occurs (step 1118). *Id.* at 14:8–34.

D. Challenged Claims

Petitioner challenges claims 1–8 and 11–18 of the '282 patent. Pet. 1. Claims 1 and 11 are independent. Claims 2–8 depend from claim 1. Claims 12–18 depend from claim 11. Ex. 1001, 16:29–18:45. Claim 1 is produced below with Petitioner's annotations to identify limitations. *See* Pet. 23–49.

1[pre] A data leak protection method comprising:
1[a][i] maintaining, by a network security device protecting an enterprise network, a filter database containing a plurality of filtering rules,
1[a][ii] wherein each filtering rule of the plurality of filtering rules specifies a watermark value, a set of network services for which the filtering rule is active and an action to be taken by the network security device,
1[a][iii] wherein the network services comprise one or more of a web-based electronic mail (email) service, Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Post Office Protocol 3 (POP3), an instant messaging program, a file sharing service and a device synchronization service;
1[b][i] receiving, by the network security device, network traffic originated within the enterprise network,
1[b][ii] wherein the network traffic is directed to a destination residing outside of the enterprise network, is associated with a particular network service and contains a file;
1[c] identifying, by the network security device, a watermark value embedded within the file;
1[d] determining, by the network security device, whether there exists a filtering rule of the plurality of filtering rules specifying a watermark value matching the watermark value embedded within the file and for which the filtering rule is active for the particular network service; and
1[e] when said determining is affirmative, then performing, by the network security device, the action specified by the filtering rule.

E. Asserted Grounds of Unpatentability

Ground	Claims	35 U.S.C. §	References
1	1, 2, 11, 12	103(a)[1]	Nagayama,[2] Crawford[3]
2	1, 2, 11, 12	103(a)	Nagayama, Crawford, Hawthorn[4]
3	3, 5–8, 13, 15–18	103(a)	Nagayama, Crawford, Sharma[5]
4	4, 14	103(a)	Nagayama, Crawford, Sharma, Wolge[6]
5	1, 2, 11, 12	103(a)	Jones,[7] Crawford
6	1, 2, 11, 12	103(a)	Jones, Crawford, Hawthorn
7	3, 5–8, 13, 15–18	103(a)	Jones, Crawford, Sharma
8	4, 14	103(a)	Jones, Crawford, Sharma, Wolge

Petitioner relies on declarations of Dr. Prasant Mohapatra. Exs. 1002, 1020.

Patent Owner relies on declarations of Dr. John Black Jr. Exs. 2001, 2004.

---

[1] The Leahy-Smith America Invents Act ("AIA") revised 35 U.S.C. § 103 effective on March 16, 2013. Changes made to 35 U.S.C. § 103 in the AIA do not apply to application for patent filed before March 16, 2013. Because the '282 patent has an effective filing date before March 16, 2013, we refer to the pre-AIA versions of 35 U.S.C. § 103.

[2] EP 1,063,833 A2, published Dec. 27, 2000 (Ex. 1003, "Nagayama").

[3] US 7,966,654 B2, issued June 21, 2011 (Ex. 1004, "Crawford").

[4] US 2013/0347085 A1, published Dec. 26, 2013 (Ex. 1005, "Hawthorn").

[5] US 2005/0271246 A1, published Dec. 8, 2005 (Ex. 1006, "Sharma").

[6] US 2010/0017436 A1, published Jan. 21, 2010 (Ex. 1007, "Wolge").

[7] US 7,298,864 B2, issued Nov. 20, 2007 (Ex. 1008, "Jones").

III. DISCUSSION

A. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art "would have had at least a B.S. in computer science, computer engineering, or electrical engineering (or equivalent experience) and at least two years of practical experience with network and data security." Pet. 16; Ex. 1002 ¶ 24. Patent Owner asserts such a person "would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master's degree in electrical engineering and/or computer science and one year of work or research experience in related fields." PO Resp. 10 (citing Ex. 2004 ¶ 18). Patent Owner also asserts that its positions "would be the same under either parties' proposal." *Id.* at 10–11 (citing Ex. 2004 ¶ 19). We adopt Petitioner's proposal with Patent Owner's contention that a master's degree in electrical engineering and/or computer science and one year of relevant experience would suffice. This level is consistent with the prior art of record and background art in the '282 patent. *See* Ex. 1001, 1:32–2:24.

B. Claim Construction

We interpret claims "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." 37 C.F.R. § 42.100(b). Under this standard, the "words of a claim 'are generally given their ordinary and customary meaning,'" as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

We construe claims only to the extent necessary to reach our decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioner "does not believe any construction is needed except 'watermark.'" Pet. 16. Patent Owner asserts that no claim terms require construction to resolve the parties' dispute. PO Resp. 11. We determine no terms require construction to reach our final written decision.

C. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103(a) if differences between the claimed subject matter 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 the subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416. The issue of obviousness is resolved based on factual determinations of (1) the scope and content of the prior art, (2) the differences between the claimed subject matter and the prior art, (3) the level of ordinary skill in the art, and (4) objective evidence of obviousness or non-obviousness. *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966). Neither party presented any objective evidence of obviousness or non-obviousness.

A party must show that a skilled artisan had a motivation to combine references and a reasonable expectation of success in doing so. *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1360–61 (Fed. Cir. 2017). A showing of reasonable expectation of success may be based on an implicit finding in view of arguments and evidence presented. *See Elekta Ltd. v. ZAP Surgical Sys., Inc.*, 81 F.4th 1368, 1376 (Fed. Cir. 2023).

D. Ground 1: Alleged Obviousness Over Nagayama and Crawford

Petitioner asserts that claims 1, 2, 11, and 12 are unpatentable under 35 U.S.C. § 103(a) over Nagayama and Crawford. Pet. 18–51.

1. Nagayama

Nagayama discloses a network security system that controls network traffic as shown in Figure 1, reproduced below. Ex. 1003 ¶¶ 1, 2, 21–23.

FIG.1

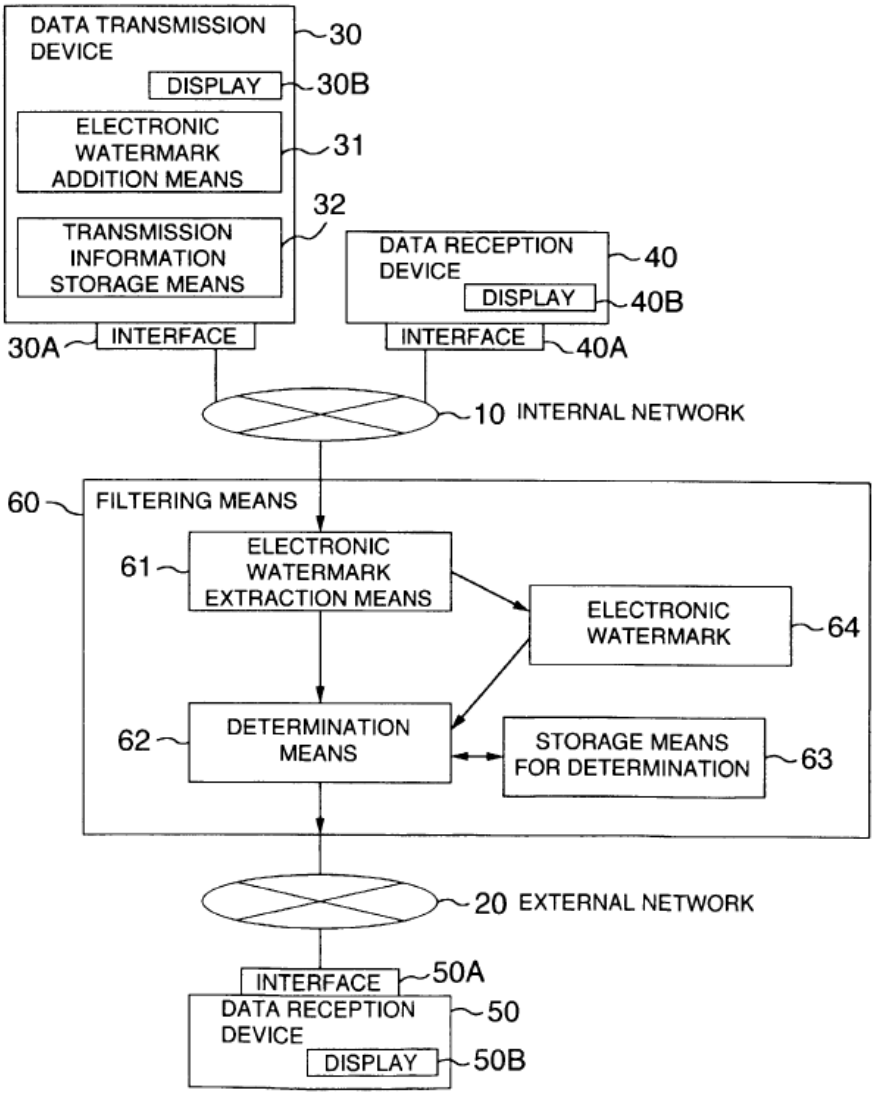


Figure 1 depicts filtering means 60 connected between an internal network 10 and external network 20 to examine data transfers between the networks and determine whether to allow transfers based on watermark information 64 contained in the data. *Id.* ¶¶ 6, 21, 23. Filtering means 60 extracts watermark information 64 embedded in received data and uses the extracted data (e.g., the type of watermark 203) to determine whether the data may be transferred to external network 20. *Id.* ¶¶ 23–25. Filter rules are stored in storage means for determination 63 and used as external transfer conditions in filtering means 60. *Id.*

Watermark data adds granularity to network data filtering. Ex. 1003 ¶¶ 24–29, 34. Figure 2 is reproduced below to illustrate the data structure of the filtering rules stored in storage means for determination 63.

FIG.2

63

205 ITEM NUMBER	201 SOURCE	202 DESTINATION	203 TYPE OF WATERMARK	204 TRANSFER ENABLE/DISABLE
1	INTERNAL	EXTERNAL	WATERMARK A	ENABLED
2	INTERNAL	DOMEIN B	NOT USED	ENABLED
3	INTERNAL	EXTERNAL	WATERMARK C	DISABLED
4	INTERNAL	EXTERNAL	NOT USED	DISABLED
...				
N	DEFAULT	DEFAULT	DEFAULT	DISABLED

Figure 2 shows an exemplary structure of storage means for determination 63, which stores data used as external transfer conditions in the filtering means 60 and includes Items/Rules 1–N. *Id.* ¶ 24. Data source 201 and data destination 202 specify sources and destinations in the internal and external networks as domain names or host names. *Id.* When specified as a domain name, data source 201 or data destination 202 indicate that a communication is from or to a computer included in that domain. *Id.* When specified as a host name, data source 201 or data destination 202 indicate a communication is from or to a computer associated with the host name. *Id.*

Type of watermark 203 indicates which type of electronic watermark information is added, and Transfer Enable/Disable 204 indicates whether the multimedia information that is embedded with an electronic watermark may be transferred depending on the determination. Ex. 1003 ¶ 24. Under the rule in Item 1, if data to be transmitted from internal source 201 to external destination 202 is embedded with Watermark A, which means "open to the outside of the company," transfer is enabled 204. *Id.* ¶ 25. The rule in Item 2 enables a transfer between internal source 201 and destination 202 in Domain B when no electronic watermark information is present in the data. *Id.* ¶ 26. Under the rule in Item 3, a transfer is disabled when source 201 is internal, destination 202 is external, and data is embedded with watermark C to indicate that the data is "confidential external to the company." *Id.* ¶ 27. Under the rule defined in Item 4, a transfer is disabled when the source 201 is internal, the destination 202 is external, and data is not embedded with electronic watermark information. *Id.* ¶ 28. Item N specifies a default case where a transfer is disabled by default when conditions in any of the item numbers above it are satisfied. *Id.* ¶ 29.

Figure 5 is reproduced below to illustrate a configuration that uses filtering means 60 in series with firewall 500. Ex. 1003 ¶ 37.

FIG.5

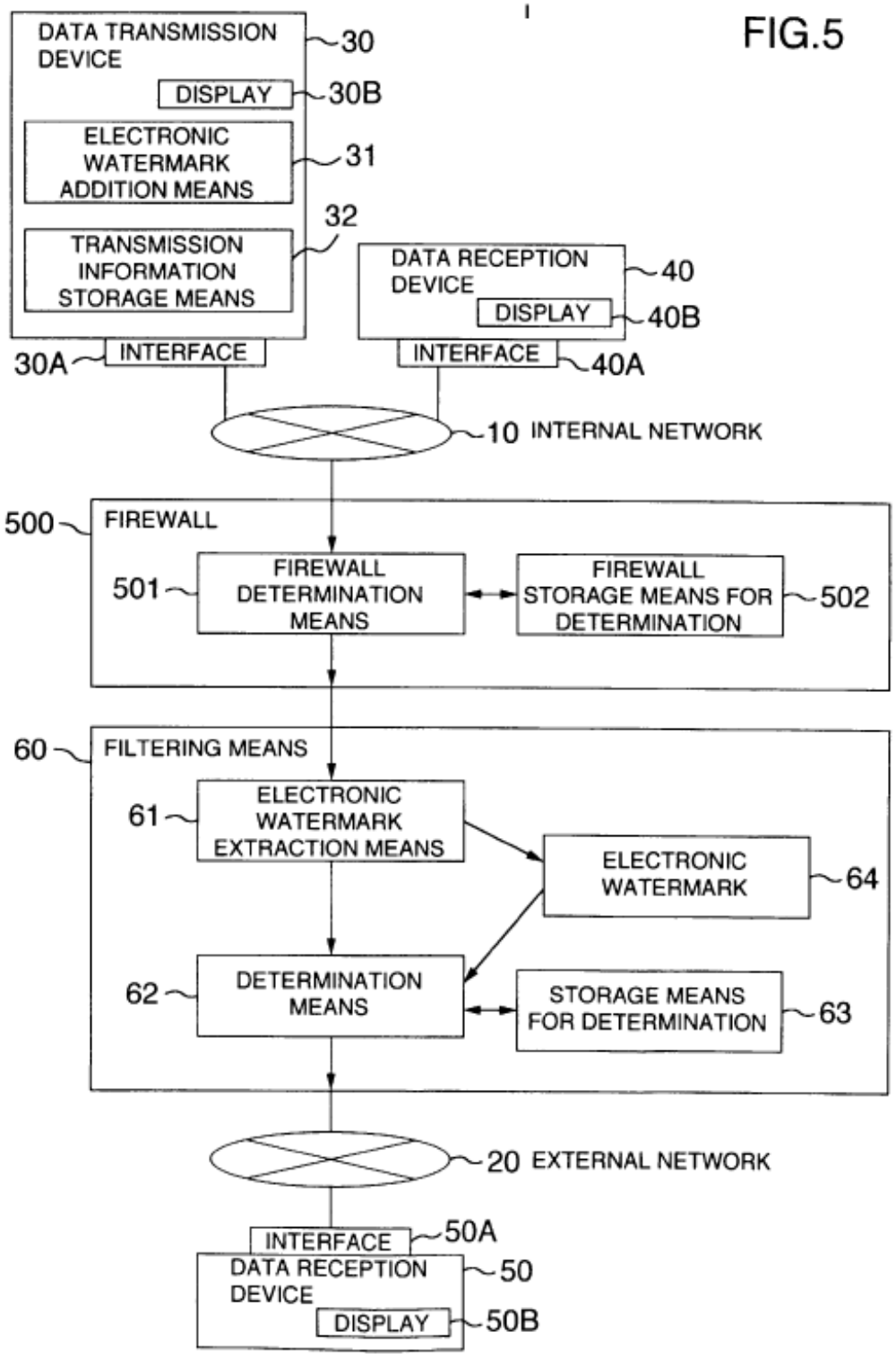


Figure 5 of Nagayama illustrates a system configuration in which filtering means 60 filters data based on electronic watermark information after the data is enabled by firewall 500 for transmission. *Id.* ¶ 37. Data to be transferred from data transmission device 30 to external data reception device 50 is first enabled or disabled by firewall 500, which determines whether to enable or disable the transfer based on the source address, the destination address, and the transfer protocol associated with the data. *Id.*

"When the transfer is enabled by the firewall 500, the data is further subjected to filtering based on an electronic watermark embedded therein" to determine whether a transfer is enabled similar to the procedure in Figure 3. Ex. 1003 ¶¶ 37, 38. Screening data at firewall 500 reduces the burden on watermark filtering means 60, which only has to filter traffic enabled at firewall 500, thereby allowing for faster filtering by requiring watermark filtering means 60 to filter only traffic enabled by firewall 500. *Id.* ¶ 38.

The positions of filtering means 60 and firewall 500 may be reversed so filtering means 60 is located nearer to internal network 10 and firewall 500 is located nearer to external network 20 so watermark filtering means 60 must permit a transfer using an electronic watermark *before* the data reaches firewall 500 for additional filtering. Ex. 1003 ¶ 39, Fig. 7. This position is effective when traffic is filtered at its destination for watermarks because the data has certain watermark information relevant to that filtering. *Id.* ¶ 39.

Firewall 810 and watermark filtering means 820 may be configured in a single device to form an integrated filtering means 800 that serves as the firewall 810 and the filtering means 820 in modular form. Ex. 1003 ¶ 39. Combining firewall 810 and filtering means 820 into a single device can improve total filtering performance. *Id.*, Fig. 8.

2. Crawford

Crawford filters network transmissions and protocols using firewall policies that improve network security. Ex. 1004, 1:6–8, 2:14–18, 6:3–45. Crawford provides more granular control over firewall settings and greater configuration flexibility. *Id.* at 4:7–12, 7:20–9:16, Figs. 3–8. Figure 5 is reproduced below to depict a table of firewall policies that includes a field identifying network services 507 for which a policy is active. *Id.* at 8:13–29.

Policy To Port External

ID	504 Source	505 Destination	506 Schedule	507 Service	508 Action	509 Configuration Scheme	510 Enable	511 Options
501 1	Internal_all	External_all	Always	Http	Allow	Scheme 3	☐	Modify Delete
502 2	MachineA	External_all	Always	Ftp	Allow	Scheme 2	☐	Modify Delete
503 5	Internal_all	External_all	Always	Any	Allow	Scheme 1	☐	Modify Delete
...	...	...	...	...	...	...	...	...

Create

Figure 5

Figure 5 depicts an interface for configuring *active* firewall policies rules 1, 2, and 5 in rows 501–503, respectively. Ex. 1004, 8:13–20. Filter policy parameters in columns 504, 505, and 507 specify a source network address, a destination network address, and a network service protocol (e.g., Http, Ftp, Any) for which each firewall filter policy is *active*. *Id.* at 8:20–23. A schedule in column 506 specifies when a policy is effective. *Id.* at 8:23–24. Column 508 specifies an Action to take for handling traffic that meets a rule. Column 509 specifies configuration schemes for each effective policy rule. Each filter rule policy may be enabled, disabled, modified, or deleted by an administrator using columns 510 and 511. *Id.* at 8:26–29.

3. Motivation to Combine and Expectation of Success

Petitioner asserts a skilled artisan would have combined Nagayama and Crawford with a reasonable expectation of success because (1) their techniques improve content filtering, (2) they each offer a content filtering system with improved flexibility, security, and convenience, and (3) filtering content by network services, as Crawford teaches, would have improved the scope, flexibility, and security of Nagayama's system by adding another, important filtering criterion in a single rule that controls access and security based on a service's vulnerability to security threats. Pet. 22–23, 28, 35–38.

Petitioner asserts that a skilled artisan would have found it obvious to filter traffic based on network services because Nagayama (1) filters traffic based on its transfer protocol (Ex. 1003 ¶¶ 37, 38), (2) filters traffic based on its destination as a *domain name or host name* (*id.* ¶ 24) and a domain name identifies a Web-based network service such as Gmail Web-based email at the domain *mail.google.com* or *gmail.com*, and (3) recognizes traffic is sent by a protocol or service, e.g., "a Web page through HTTP or the like" or "a mail or the like" (*id.* ¶ 32) so a skilled artisan would have found it obvious to filter network traffic using host or domain names *and network services*. Pet. 22–23, 35–36. Petitioner asserts a skilled artisan would have filtered traffic by network services in Nagayama based on Crawford's teachings to filter network services. *Id.* at 36–38. Dr. Mohapatra's testimony supports these assertions. Ex. 1002 ¶¶ 94–97, 119–128 (cited in Pet. 22–23, 35–38).

We determine that Petitioner has shown by a preponderance of the evidence that a skilled artisan would have been motivated to combine the teachings of Nagayama and Crawford with a reasonable expectation of success as set forth above and discussed in § III.D.4.c. and § III.D.4.d. *infra*.

4. Independent Claims 1 and 11

a. 1[pre]/11[pre]: "A data leak protection method comprising:/A non-transitory program storage device readable by a network security device . . . to perform a method of data leak protection . . . comprising:"

Petitioner asserts that Nagayama discloses a method for "protecting particular data from leaking from an internal network to the outside" and "for filtering particular data in such a manner that data embedded with an electronic watermark [was] not open to the outside." Pet. 23–24 (citing Ex. 1003 ¶¶ 1, 5, 44; Ex. 1002 ¶¶ 98, 99, 101). Petitioner contends that Nagayama uses a network security device (filtering means 60) to prevent content from leaking from an internal enterprise network to an external network due to unauthorized transfers by extracting electronic watermark information 64 embedded in received data and using that information to determine whether the data may be transferred to external network 20.

Petitioner asserts that Nagayama's filtering means 60 uses watermark extraction means 61, storage means 63 that stores transfer conditions, and determination means 62 that determines if data can be transferred based on watermark data and transfer conditions, and it can be implemented in a computer readable storage medium such as a server or hard drive. Pet. 24–25 (citing Ex. 1003 ¶¶ 1, 5, 6, 11, 21, 23, 24, 44, claim 6, Fig. 1; Ex. 1002 ¶¶ 100–105; Ex. 1001, 5:10–14, Fig. 1).

Patent Owner does not challenge these contentions. *See generally* PO Resp.; Sur-reply. Regardless of whether the preamble is limiting, based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama and Crawford teach or suggest elements 1[pre]/11[pre].

b. 1[a][i]/11[a][i]: "maintaining, by a network security device protecting an enterprise network, a filter database containing a plurality of filtering rules"

Petitioner contends that Nagayama's filtering means 60 protects an enterprise network using a storage means of transfer conditions (rules) in a table (database) to determine information that can be transmitted externally. Pet. 26–28 (citing Ex. 1003 ¶¶ 24, 26–28, Figs. 1, 2; Ex. 1002 ¶¶ 106–111).

Patent Owner does not challenge these contentions. *See generally* PO Resp; Sur-reply. Based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama and Crawford teach or suggest elements 1[a][i]/11[a][i].

c. 1[a][ii]/11[a][ii]: "wherein each filtering rule of the plurality of filtering rules specifies a watermark value, a set of network services for which the filtering rule is active and an action to be taken by the network security device,"

Petitioner asserts that Nagayama's transfer rules specify a watermark value of sensitivity level (e.g., copyright, confidentiality) and source, origin, owner, or company identifier and an action to take by the filtering means to enable or disable a transfer based on analysis of the source, destination, and watermark value. Pet. 28–32 (citing Ex. 1003 ¶¶ 19, 24, 27, 34, Fig. 2; Ex. 1002 ¶¶ 112–115; Ex. 1001, 1:51–54). Petitioner asserts that the '282 patent describes network services as applications (Yahoo! Mail, Gmail, MSN mail) and protocols (IMAP, POP3), and Nagayama filters traffic based on its protocol and destination and recognizes traffic is associated with a protocol or service (e.g., a Web page via HTTP or mail). Pet. 32–36 (citing Ex. 1003 ¶¶ 24, 32, 37, 38; Ex. 1001, 13:8–11, Figs. 9, 10; Ex. 1002 ¶¶ 116–120).

Petitioner asserts that a skilled artisan would have found it obvious to filter traffic based on a network service in its filter rules because Nagayama filters traffic based on its destination identified by host or domain name that could identify a network service such as Gmail, its associated protocol or service such as a Web page through HTTP, or a mail or the like. Pet. 35–36 (citing Ex. 1003 ¶¶ 24, 32, 37, 38; Ex. 1002 ¶¶ 119–120). Petitioner asserts that Crawford filters network traffic using rules that filter a set of network services such as "*at least one* service network protocol" or "Any" network service (Rule 5) that includes "Http" and "FTP" in Rules 1 and 2 of a table of filter rules, and Crawford recognizes network applications use multiple protocols that are related. *Id.* at 36–39 (citing Ex. 1004, 2:24–28, 2:48–51, 7:46–47, 9:10–13, Fig. 5; Ex. 1003 ¶ 25; Ex. 1002 ¶¶ 121–128).

i. Patent Owner's arguments

Patent Owner argues that Petitioner fails to explain why a skilled artisan would have modified Nagayama's watermark filtering means to filter traffic based on watermarks and network services when Nagayama filters network traffic based on transfer protocol using a firewall. PO Resp. 12–13. Patent Owner also asserts that "Nagayama teaches away from Petitioner's proposed combination [because] in every embodiment in which Nagayama's communication system filters data based on transfer protocol, Nagayama . . . implements the transfer protocol-filtering device as either physically or functionally *separate* from the watermark filtering means." *Id.* at 14. Patent Owner argues that Nagayama intentionally separates firewall and watermark filtering as separate modules that perform their functions serially to reduce a burden on the filtering means, and contradicts Petitioner's reason to modify the watermark filtering means to filter for network services. *Id.* at 15–19.

ii. *Analysis*

We disagree with Patent Owner's arguments for the following reasons.

(a) Nagayama's Figure 1 embodiment does not include a firewall as Patent Owner asserts

Petitioner asserts that Nagayama's filtering means 60 in Figure 1 is a network security device for element 1[a][i]/11[a][i]. Pet. 26–27. Filtering means 60 includes watermark extraction means 61 to extract watermarks 64 from received data and storage means for determination 63 to store filtering rules that specify data source 201, data destination 202, watermark type 203, and action to take 204. *Id.*; Ex. 1003 ¶¶ 23, 24. Filtering means 60 is not used with a firewall. Ex. 1003 ¶¶ 21–24, Figs. 1–3. We find that Patent Owner's teaching-away argument is inapplicable to Petitioner's combination of Nagayama's *Figure 1 embodiment* with Crawford because watermark filtering means 60 is not used with a firewall. *Id.*; *see* PO Resp. 12–14.

We agree with Petitioner that it would have been obvious to add network services in Nagayama's table of filter rules to filter traffic by its network protocol because (1) Nagayama filters traffic based on its protocol in some embodiments, (2) Nagayama's filter rules specify a destination that can be a domain name that identifies a network service such as Gmail Web-based email service at *mail.google.com*, (3) Nagayama recognizes that the traffic can relate to "a Web page through HTTP or the like" or "a mail or the like," and (4) Crawford's filter rules include network services with source and destination that would improve the security, flexibility, and granularity of Nagayama's database of filter rules similarly. Pet. 35–36 (citing Ex. 1003 ¶¶ 24, 32, 37, 38; Ex. 1002 ¶¶ 119, 120).

(b) Nagayama's watermark-firewall embodiments

For Nagayama's embodiments that use watermark filtering means 60 with a firewall, we disagree with Patent Owner's teaching-away arguments for other reasons. Nagayama describes embodiments that place watermark filtering means 60 in series with firewall 500 so traffic from internal network 10 is filtered and enabled by firewall 500 based on transfer protocols before it is filtered by watermark filtering means 60. Ex. 1003 ¶¶ 37, 38, Figs. 5, 6. This arrangement may be integrated as filtering means 800. *Id.* ¶ 39, Fig. 8. Nagayama's teachings of alternative embodiments do not "teach away" from any of Nagayama's embodiments. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004) ("The prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the [claimed] solution."); *see* Reply 6.

Indeed, we find that adding network services to Nagayama's filtering rules *further reduces* the filtering burden on Nagayama's watermark filter. Watermark filter 60 only filters traffic *for watermarks* if its watermark filter rules are *active* for the network service associated with the traffic. It does not watermark filter all the network traffic that a firewall enables to reach it.

This modification to Nagayama's database filter rules is consistent with Nagayama's embodiments that use firewalls 500, 810 in series with watermark filtering means 60, 810 to reduce the burden on filtering means 60, 810 by first disabling traffic at a firewall based on the network protocol associated with the traffic so the watermark filtering means does not have to examine that traffic for watermark payloads using its more time-consuming watermark filtering techniques. Ex. 1003 ¶¶ 37, 38.

Petitioner modifies Nagayama's *database of filter rules* to make rules active for certain network services associated with network traffic. Pet. 38. Making Nagayama's filter rules *active* for certain network services *reduces the burden on the watermark filter* because it (1) does not filter traffic that is disabled by a firewall based on its network service as Nagayama teaches *and* (2) it does not filter other traffic sent by network services for which it has *no active filter rules*. We do not agree with Patent Owner that there is a "tradeoff." Reply 6–9; *cf.* PO Resp. 15–19, 22–23. Petitioner illustrates the change to Nagayama's database of filter rules in a table reproduced below.

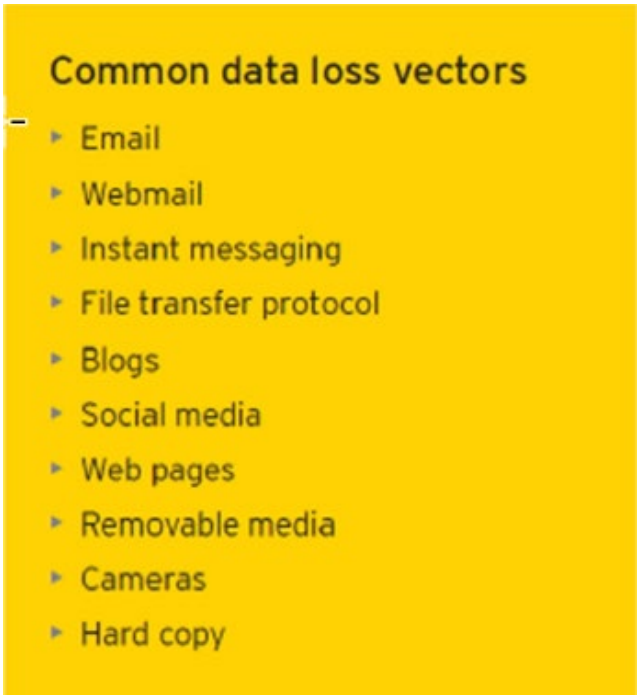
Nagayama and Crawford Combined

ITEM NUMBER	SOURCE	DESTINATION	TYPE OF WATERMARK	NETWORK SERVICE	TRANSFER ENABLE/DISABLE
1	INTERNAL	EXTERNAL	WATERMARK A	GMAIL, IMAP, SMTP, POP3	ENABLED
3	INTERNAL	EXTERNAL	WATERMARK C	DROPBOX, FTP, BITTORRENT	DISABLED

Pet. 38. As shown in the table, Petitioner has modified Nagayama's table of watermark filtering rules to add a "Network Service" field to improve security, flexibility, and granularity of Nagayama's network traffic filtering for DLP. *Id.* We agree with this analysis by Petitioner. Nagayama's *data leakage triage* process is extended and enhanced for greater granularity and flexibility *and speed* by considering network services. The need for time-consuming watermark filtering is reduced to the minimum by only filtering files sent by network services for which there is an active rule in the table. Thus, we do not credit Dr. Black's testimony that the change overburdens the watermark filtering means and teaches away. Ex. 2004 ¶ 47.

(c) Nagayama's filter rules include watermark values and network services in a single rule

We find that adding network services to Nagayama's database of filter rules improves network security, flexibility, and granularity by filtering traffic by source and destination, watermark values, *and* network protocols in a *single filter rule*, and the improvement provides a motivation to combine the teachings of Nagayama and Crawford. *See* Pet. 22–23, 35–39; *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (an implicit motivation to combine exists when an improvement makes a product stronger, cheaper, faster, lighter, smaller, more durable, or more efficient). *A single rule* provides granular analysis of network services identified as common data loss vectors in a 2011 report reproduced below when data is sent from a secure internal network to a less insecure external network in Nagayama. Reply 14; Dec. Inst. 30–31, 34; Ex. 1003 ¶¶ 1, 5, 6, 21, Fig. 1; Pet. 18–22; Ex. 1002 ¶¶ 51, 96.



The "Common data loss vectors" are identified in an Ernst & Young report on *Data Loss Prevention*. Ex. 1002 ¶ 51 & n.19; Reply 3. Petitioner asserts that "those vectors align with the claimed network services [so] a [skilled artisan] would be motivated to filter by them." Reply 3; *id.* at 12–13.

This report supports Dr. Mohapatra's testimony that industry is aware that the uncontrolled, unmonitored use of email, instant messaging, website forms, file transfers, and other outgoing traffic creates a risk that confidential information will fall into the wrong hands and harm businesses. Ex. 1002 ¶¶ 51, 53. This report and Dr. Mohapatra's testimony provide a persuasive reason why an ordinarily skilled artisan would have added network services to Nagayama's database of filter rules. We agree with his testimony that adding network services as a field in a single rule leverages Crawford's teachings to filter specific protocols with other parameters, and it would improve the filtering flexibility and security of Nagayama by filtering network services with known vulnerabilities to data leakage. *Id.* ¶ 96.

(d) Improved security, flexibility, convenience

As we preliminarily determined in our Decision on Institution, we find that adding network services as a field to Nagayama's database of filter rules yields predictable results of more security, flexibility, and granularity as the references teach. Dec. Inst. 30–34. We find that filtering traffic based on watermarks for different confidentiality and security levels in Nagayama and for security based on network services in Crawford would be improved by a *single rule* for watermarks and network services to avoid blind spots. *Id.* at 32–34. We agree that Crawford uses network protocols to improve security and flexibility by taking appropriate action for a protocol for various security threats. Ex. 1004, 1:35–2:58, 4:7–57, 6:3–45, 7:20–8:3, 8:36–53.

We find that Crawford's use of network service protocols to filter traffic would have improved Nagayama's filtering flexibility by modifying Nagayama's filtering rules to filter for network service protocols. Like Crawford's proxy servers, Nagayama's watermark filter permits deeper examination of files to identify and extract watermarks for more granularity, flexibility, and security of data leakage filtering. Ex. 1003 ¶¶ 5, 6, 19, 25–27; *cf.* PO Resp. 34–35. The flexibility and granularity of data leakage protection and security that the Nagayama–Crawford combination would have provided is enhanced by their complementary techniques for achieving predictable results by using network protocols as a parameter in Nagayama's watermark filter rules, as Dr. Mohapatra testifies. Ex. 1020 ¶¶ 9–12, 16–21.

We find Crawford's teaching that "[t]he configuration database . . . may be as simple as a text file holding records of information or as complex as a fully featured database system" supports the combination (Ex. 1004, 5:15–18) as does its teaching that "[v]arious other settings and parameters may be displayed and appropriately configured" (*id.* at 7:63–65). We find that Crawford's teachings address "blind spots" discussed by Dr. Mohapatra by filtering email (e.g., SMTP, IMAP, POP3) so security is enhanced with multiple configuration settings for each specific protocol. *Id.* at 7:29–8:3, 9:1–27, Figs. 5, 7–9; *see* Reply 22–23. We find that the prior art establishes that filtering network traffic by parameters such as network services would have improved the security, granularity, and flexibility of those systems to protect networks and prevent data leaks, and Crawford describes the ease with which network services are identified by network service port identifiers in packets so implementation would have been within the level of ordinary skill and predictable. Ex. 1004, 4:24–35; *see* Reply 27–28.

Dr. Mohapatra also testifies that a skilled artisan would have filtered multiple network services in a single rule based on Crawford's teachings and the knowledge in the art that a file transfer service includes multiple services such as FTP, telnet, and bit-torrent, "network services" include *applications* like Gmail and *protocols* like IMAP, and network services can use multiple protocols such as IMAP and POP3 protocols for Gmail. Ex. 1002 ¶¶ 122–125. We credit his testimony that such filtering "would help avoid blind spots in the system" by filtering multiple protocols used by the system to provide a consistent way to screen content prior to transmission outside the company with a watermark value in all filtering rules. *Id.* ¶¶ 124–127.

(e) Secure versus unsecure network protocols

Patent Owner also argues that filtering network services by secure and unsecure protocols does not address Nagayama's concern that data leakage occurs at a destination after data is decrypted so secure network protocols are "highly susceptible to leakage." PO Resp. 19–20. We disagree.

This argument ignores the fact that Nagayama uses a watermark filter to prevent certain files with particular watermarks from reaching an external network where they can be decrypted. Noting this problem (Ex. 1003 ¶ 4), Nagayama "protect[s] particular data from leaking from an internal network to the outside without preventing information from being opened to internal users" (*id.* ¶ 5) "by examining whether the data transfer satisfies conditions defined by the contents of an electronic watermark included in the data" (*id.* ¶ 6), and "determining whether or not a transfer of the data to another information processing device is enabled or disabled by examining extracted information" (*id.* ¶ 11). Petitioner's combination retains Nagayama's ability to prevent data leakage to destinations by filtering watermarks. Pet. 28–38.

We find that Petitioner's modification would have enabled Nagayama to prevent data leakage that could occur if sensitive data was sent over the Internet or other network using an unsecure network protocol where it might be intercepted *in transit* and compromised by risky data loss vectors. Reply 1–3; Ex. 1020 ¶¶ 6–10; Ex. 1002 ¶¶ 51, 96, 134. Patent Owner's arguments do not address Petitioner's contentions in these regards or their discussion of HTTPS/HTTP as *exemplary* of this data leakage issue. Dec. Inst. 47.

(f) "a set of network services"

Patent Owner argues that Crawford's filtering rules do not specify "a ***set*** of network services" because Crawford's application of a filter rule to "Any" services "is the same thing as a filter rule that specifies *no* network service." PO Resp. 36–37. Patent Owner argues that Rule 5's specification of "Any" network service protocols specifies no network services. *Id.* at 37.

We disagree. The claim language does not prevent "a set of network services" from comprising a single network service if an administrator so desires. The '282 patent describes an interface where an administrator can designate *one or more* network services for a filter rule. Ex. 1001, 13:5–13, Fig. 9. Thus, the plain meaning of the claim language and specification indicate "a set of network services" may be more than one network service *or a single network service* as an administrator chooses.

We find that Crawford allows an administrator to specify a single network service for a filter rule (e.g., HTTP, FTP) or "Any" network service, which teaches more than one network service (e.g., HTTP, FTP, and/or another network service) *and suggests* a rule may encompass a set of more than a single network service, as Petitioner asserts. Pet. 37–38. We disagree that "Any" services means no services, as Patent Owner argues.

Crawford teaches that certain network service protocols have common filtering concerns. Thus, SMTP, IMAP, and POP3 use the same filtering rule of AV Scan, File Block, and Spam block. Ex. 1004, 9:1–7, Fig. 7. The same rule can be applied to a *set* of email protocols. These teachings also support our determination that it would have been obvious to modify Nagayama's database to specify a filter rule for "a set of network services."

Crawford discloses different configurations for different protocols as Patent Owner asserts, because email spam block may not be appropriate for non-email protocols. PO Resp. 37–38; Ex. 1004, 7:43–47. This teaching indicates the same filter rule may be appropriate for a set of *similar* network services such as SMTP, IMAP, and POP3. Ex. 1004, 9:1–16, Figs. 7, 8 (SMTP, IMAP, and POP3 use the same settings of antivirus scan, filename block, and pass fragmented emails). We find that the teaching of common filtering vulnerabilities/needs of email network services teaches and suggests a single rule would have been desirable for a set of such network services.

We credit Dr. Mohapatra's testimony that Crawford teaches that "[t]he inventive firewall policy includes . . . ***at least one*** service network protocol" and Rule 5 in Figure 5 indicates its applicability to "Any" network service that would include at least HTTP in Rule 1 and FTP in Rule 2 of that table of filtering rules. Ex. 1002 ¶ 122 (citing Ex. 1004, 2:48–51).

(g) No tradeoff(s) is required or asserted

We disagree with Patent Owner's argument that adding network services to Nagayama's filtering rules would have resulted in a tradeoff in efficiency because Nagayama divides network security between firewall 810 and watermark filtering means 820 to perform data leakage and security sequentially to enhance filtering efficiency and speed. Ex. 1003 ¶¶ 37, 38.

We find that this configuration would have *decreased* the amount of watermark filtering that the watermark filter performed. The *burden* on the watermark filter would have been *reduced*. *Cf.* PO Sur-reply 7–8. Making watermark filtering rules active only for some network services would have reduced the need for watermark filtering. Ex. 1003 ¶ 38, Fig. 6 (604). The "tradeoff" would have been more efficient, streamlined filtering that applies watermark filtering only to network traffic that is enabled by a firewall *and* covered by an "active" watermark filtering rule. Just as files with particular watermark values may be permissible to send between certain sources and destinations (Ex. 1003 ¶¶ 24–28), they also may be permissible to send over some network services and not others (Ex. 1002 ¶¶ 51–73, 96) for security.

Watermark filtering focuses on network traffic that is prone to leakage or that presents DLP security concerns. Ex. 1003 ¶¶ 5–12. The more time-intensive watermark filtering is limited to situations where it is needed, and other network traffic may be disabled at a firewall to prevent data leakage in a data leakage triage configuration. *Id.* ¶¶ 4–13, 23–28, 37–38. Not filtering traffic sent by network services that do not require watermark filtering does not undermine network security as Patent Owner asserts. PO Resp. 19–22.

Using a single rule to filter network traffic by watermark value and network service would have added flexibility and security, e.g., by applying watermark filtering to traffic sent by less secure protocols that are prone to data leakage (Pet. 23) or network services that are appropriate or acceptable for internal rather than external network traffic (Ex. 2007, 106:13–107:8). Simply put, certain watermarked files may not be appropriate for external transmission using certain network services, and a *single filter rule* can make that distinction. Pet. 22–23, 28–39; Reply 2–4, 15; Dec. Inst. 31–34.

We find that Nagayama's Figure 7 embodiment is not cited to show it would have been obvious to use a single watermark filtering rule that is active for particular network services. Reply 6–7, 8–9; Pet. 28–39; PO Sur-reply 6–7. Nagayama teaches, "[t]his positioning is effective *when data is filtered at its destination* on the assumption that the data has certain electronic watermark information." Ex. 1003 ¶ 39 (emphasis added).

(h) Conclusion

For the reasons given, Petitioner's has established by a preponderance of the evidence that Nagayama and Crawford teach and suggest elements 1[a][ii]/11[a][ii].

d. 1[a][iii]/11[a][iii]: "wherein the network services comprise one or more of a web-based electronic mail (email) service, Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Post Office Protocol 3 (POP3), an instant messaging program, a file sharing service and a device synchronization service;"

Petitioner contends that elements 1[a][iii]/11[a][iii] recite a non-exhaustive list of well-known network service protocols and applications, and Crawford discloses the use of its system with a similar variety of well-known protocols and applications that include SMTP, IMAP, POP3, instant messaging program, file sharing service, and device synchronization service and associated applications such as Web browsers, email, and telnet that would include well-known Web-based emails like Gmail and Yahoo! Mail. Pet. 39–41 (citing Ex. 1004, 1:38–40, 6:3–16, 7:46–47; Ex. 1002 ¶¶ 129–134; Ex. 1005 ¶ 24; Ex. 1009, 4 ("BitTorrent" definition), 8 ("IMAP" definition)).

Petitioner also asserts that network services like the claimed SMTP, POP3, IMAP, FTP, and instant messaging have security vulnerabilities such that secure versions of these network services were created as SMTPS, POP3S, IMAPS, FTPS/SFTP as Patent Owner's expert, Dr. Black, admits. Petitioner asserts that a skilled artisan would have been motivated to restrict sensitive information from being transmitted over these unsecure protocols for the reasons explained for HTTP and HTTPS, which is exemplary of this security problem. Reply 2 (citing Dec. Inst. 35; Pet. 23, 66; Ex. 1002 ¶¶ 73, 96, 188; Ex. 1020 (Dr. Mohapatra Rebuttal Declaration) ¶¶ 6–10; Ex. 1014 (Dr. Black Deposition), 10:8–11:17, 13:9–14:8, 14:23–15:5, 17:3–5; Exs. 1016–1018; Ex. 1019, 146).

Petitioner contends that these claimed network services are recognized as common data loss vectors because they are avenues for data leaks so that a skilled artisan would have been motivated to filter network traffic for these network services and block network traffic associated with these network services to prevent data leaks. Reply 2 (citing Pet. 9, 23; Ex. 1002 ¶¶ 51 (citing *Data Loss Prevention*, Ernst and Young (2011) that lists "[c]ommon data loss vectors" as being email, Webmail, instant messaging, File Transfer Protocol, social media, Web pages, and blogs), 96, 134; Ex. 1020 ¶ 11).

Petitioner also contends that combining Crawford's teaching to filter network traffic associated with particular network services with Nagayama "provides improved flexibility and convenience, as the Board already found" and "a [skilled artisan] would want the flexibility to specify only network services appropriate for a rule (e.g., identifying all email-related network services) and the convenience of doing so in a single-filter rule." Reply 4 (citing Dec. Inst. 29–30; Pet. 11, 22–23; Ex. 1015, 35; Ex. 1020 ¶ 12).

i. Patent Owner's arguments

Patent Owner asserts that for limitation 1[a][ii], Petitioner argued that network services like HTTP that support Web-based email were known to be more vulnerable to security threats so a skilled artisan would have wanted to provide different access or security control measures for those services (Pet. 23), but for limitation 1[a][iii], "Petitioner makes no showing that any of the listed network services suffer from security vulnerabilities" (*id.* at 39–41). Patent Owner asserts that providing different access or security control measures for network services with security vulnerabilities does not explain why a skilled artisan would have been motivated to filter data based on the claimed network services. PO Resp. 39–40.

ii. Analysis

We find that Petitioner has shown that a skilled artisan would have filtered these network protocols to address known security vulnerabilities. As we discussed in our Decision on Institution, Petitioner cited HTTP as an *example* of a network service that has known security vulnerabilities as also evidenced by the fact that a more secure version (i.e., HTTPS) has been developed to address some of the known security vulnerabilities in HTTP. As a result, we preliminarily found that filtering traffic for network protocols that have such known security vulnerabilities improves security. Dec. Inst. 35. In response to Patent Owner's arguments, Petitioner provided evidence that more secure versions of other network services that have some security vulnerabilities, such as Web-based email, SMTP, IMAP, POP3, and FTP, were developed as SMTPS, POP3S, IMAPS, and FTPS/SFTP to address the "prevalence of intercepted data" that causes data leaks when the less secure versions of these network service protocols are used. Reply 2.

Our determination is supported by Dr. Black's testimony. Dr. Black testifies that a more secure version of SMTP was developed as SMTPS that encrypts data rather than sending it as plain text as occurs with the less secure SMTP network protocol. Ex. 1014, 13:9–14:8. Dr. Black testifies that a more secure version of FTP was developed as FTPS, which provides an encryption authentication protocol that improves the security of FTP, which sends data in a less secure plain text format. *Id.* at 14:10–17:5.

We credit Dr. Black's testimony, which evidences the knowledge in the art that different network service protocols include different security features that provide different levels of network security so a skilled artisan would have been motivated to filter different network services that provide different security levels and different security vulnerabilities differently to prevent or reduce data leakage. Different filter rules are used for different network services, as appropriate, depending on the security level and the confidentiality of data sent, as Nagayama and Crawford both recognize. Ex. 1004, 4:8–42, 7:43–8:3, 9:1:27; Ex. 1003 ¶¶ 24–29, 33, 37, 38, Fig. 2.

To prevent data leaks, an enterprise may filter files containing certain watermarks sent by unsecure network services of SMTP, IMAP, POP3, and FTP but allow such files to be sent over more secure network services of SMTPS, IMAPS, POP3S, and FTPS. *See* Reply 2–4; *KSR*, 550 U.S. at 417.

We agree with Petitioner that making Nagayama's watermark filtering rules active for certain network services would have improved flexibility, granularity, and security depending on an entity's DLP policies and would have reduced the burden on the watermark filter. Reply 4–7. This rationale supports the proposed modification of Nagayama's database of filter rules for elements 1[a][ii]/11[a][ii] and elements 1[a][iii]/11[a][iii].

Data with different confidentiality would be filtered by watermarks, source and destination addresses, and network services for its vulnerabilities and other security factors for greater granularity and flexibility, as explained in our Decision on Institution. Dec. Inst. 29–34; Pet. 18–23, 28–41.

iii. Conclusion

For the reasons given, Petitioner has established by a preponderance of the evidence that Nagayama and Crawford teach and suggest elements 1[a][iii]/11[a][iii].

e. 1[b][i]/11[b][i]: "receiving[, by the network security device,] network traffic originated within the enterprise network,"

i. Petitioner's contentions

Petitioner contends that Nagayama's filtering means receives network traffic that originates from within an internal enterprise network such as data transmission device 30 in internal network 10 transmitting data such as email through filtering means 60 located outside internal network 10. Pet. 41–43 (citing Ex. 1003 ¶¶ 32, 34, Figs. 1, 3; Ex. 1002 ¶¶ 135–137). In addition, Dr. Mohapatra testifies that these elements are disclosed in Nagayama as combined with the teachings of Crawford. Ex. 1002 ¶ 137.

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[b][i]/11[b][i]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama discloses elements 1[b][i]/11[b][i].

f. 1[b][ii]/11[b][ii]: "wherein the network traffic is directed to a destination residing outside of the enterprise network, is associated with a particular network service and contains a file;"

i. Petitioner's contentions

Petitioner asserts that Nagayama and Crawford send traffic/a file to an external device and link traffic to a network service. Pet. 43–44 (citing Ex. 1003 ¶¶ 22, 32–34, 37, 38; Ex. 1004, 6:3–5, 9:32–37; Ex. 1002 ¶¶ 138–141).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[b][ii]/11[b][ii]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama and Crawford disclose and suggest elements 1[b][ii]/11[b][ii].

g. 1[c]/11[c]: "identifying[, by the network security device,] a watermark value embedded within the file;"

i. Petitioner's contentions

Petitioner contends that Nagayama's filtering means 60 identifies a watermark embedded in network traffic using watermark extraction means 61 to "*acquire electronic watermark information possibly embedded in the received data (step 305)*" where the watermark extraction means is part of the watermark filtering means, which provides the network security device. Pet. 44–45 (citing Ex. 1003 ¶ 33, Figs. 1, 3; Ex. 1002 ¶¶ 142–145).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[c]/11[c]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama discloses elements 1[c]/11[c].

h. 1[d]/11[d]: "determining[, by the network security device,] whether there exists a filtering rule of the plurality of filtering rules specifying a watermark value matching the watermark value embedded within the file and for which the filtering rule is active for the particular network service;"

i. Petitioner's contentions

Petitioner asserts that Nagayama's watermark filtering means extracts a watermark value and determines whether it matches a value in a filter rule, but Nagayama does not determine whether the filtering rule is active for the particular network service. Petitioner contends that a skilled artisan would have found it obvious to make Nagayama's filter rules active for network services based on Crawford's teachings because Nagayama filtered traffic based on its network protocol, and Crawford associated network protocols with traffic to improve Nagayama's filtering means to determine whether a watermark filtering policy applied to outgoing traffic by using the additional metric of a network service protocol. Pet. 45–48 (citing Ex. 1003 ¶¶ 23, 27, 33, 37, 38, Figs. 2, 3; Ex. 1004, 9:18–27, Fig. 9; Ex. 1002 ¶¶ 146–152).

ii. Patent Owner's arguments

Patent Owner asserts the same arguments for elements 1[d]/11[d] as Patent Owner asserted for elements 1[a][ii]/11[a][ii]. *See* PO Resp. 12–39. We addressed these arguments in Section III.D.4.c. *supra* for elements 1[a][ii]/ 11[a][ii]. We disagree with Patent Owner's arguments for elements 1[d] 11[d] for the same reasons set forth in Section III.D.4.c. *supra*.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama and Crawford disclose or suggest elements 1[d]/11[d].

i. 1[e]/11[e]: "when said determining is affirmative, then performing[, by the network security device,] the action specified by the filtering rule."

i. Petitioner's contentions

Petitioner asserts that Nagayama's filtering means takes action set by a rule when traffic matches a transfer rule such as enabling a data transfer if the determination indicates the transfer is enabled or blocking a data transfer if the determination indicates the transfer is disabled as shown in the table reproduced below with "Network Service" added as a filter field. Pet. 49–50 (citing Ex. 1003 ¶¶ 11, 27, 33, Fig. 3; Ex. 1002 ¶¶ 153–156).

Nagayama and Crawford Combined

ITEM NUMBER	SOURCE	DESTINATION	TYPE OF WATERMARK	NETWORK SERVICE	TRANSFER ENABLE/DISABLE
1	INTERNAL	EXTERNAL	WATERMARK A	GMAIL, IMAP, SMTP, POP3	ENABLED
3	INTERNAL	EXTERNAL	WATERMARK C	DROPBOX, FTP, BITTORRENT	DISABLED

The table above shows a database of filter rules of Nagayama as modified by Crawford's teachings to filter network traffic based on network services to enhance security, flexibility, and granularity as discussed above. Pet. 38, 50. Rule 3 of the table shows traffic disabled when it contains watermark C and is associated with Dropbox, FTP, or BitTorrent network services. *Id.* at 50.

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding elements 1[e]/11[e]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Nagayama and Crawford disclose or suggest elements 1[e]/11[e].

j. Reasonable Expectation of Success

i. *Petitioner's contentions*

Petitioner asserts that a skilled artisan would have combined Crawford and Nagayama with a reasonable expectation of success because they both improve content filtering, and Nagayama filters content based on a source, destination, watermark, and associated protocol but not specific protocols, and Crawford filters traffic by network service. Pet. 22–23 (citing Ex. 1002 ¶¶ 95–96). Petitioner asserts that these software functions require only code to be written within the level skill of the art. Reply 27 (citing *Keynetik, Inc. v. Samsung Elec. Co.*, 2023 WL 2003932, at *2 (Fed. Cir. Feb. 15, 2023)).

Petitioner asserts that modifying Nagayama to filter traffic by network service would have been simple and straightforward where (1) the references maintain a database of filtering rules, (2) they improve content filtering, (3) creating filtering rules that specify watermarks and network services was known, (4) filtering traffic by protocol was done by the earliest firewalls, (5) protocols had well-known port numbers associated with them, (6) packet inspection was well-known, and (7) Nagayama already disclosed the concept of filtering network traffic by network service protocols. Reply 27–28. Petitioner asserts that it showed how network services could be identified in Nagayama's filtering rules, and Patent Owner does not dispute this evidence, argue unpredictability in combining references, or assert that a skilled artisan would have lacked the skill to make the proposed combination. *Id.* at 28.

ii. Patent Owner's arguments

Patent Owner argues that Petitioner provides a conclusory assertion. PO Resp. 44. Patent Owner asserts that Dr. Mohapatra "is completely silent on the issue." *Id.* (citing Ex. 1002 ¶¶ 94–97). Patent Owner argues that a skilled artisan would not have had a reasonable expectation of success based on Nagayama's teachings because its watermark filter means takes a "long time" and should not be burdened with filtering data based on a transfer protocol. *Id.* at 45 (citing Ex. 1003 ¶ 38). Patent Owner asserts that

> a [skilled artisan] would have had serious concerns that modifying Nagayama's watermark filtering means to additionally filter data based on network services would introduce an unreasonable amount of network latency or otherwise frustrate the operability of Nagayama's communication system. Avoiding bottlenecks at network devices that serve as critical gateways through which all data must pass between an internal and external network, such as Nagayama's watermark filtering means, is crucial for the practical operability of a communication system.

Id. Patent Owner argues that these network delays would have frustrated Nagayama's intended purpose even if a skilled artisan could have modified Nagayama's watermark filtering means' database of filter rules to include an additional column for network services. *Id.* at 46.

iii. Analysis

We find that Petitioner has established a reasonable expectation of success in combining the relevant teachings of Nagayama and Crawford. As discussed in Section III.D.4.c. *supra*, claims 1 and 11 require the network security device (watermark filter) to identify a watermark value in the file; they do not require the network service device to *identify* a network service. The claims do not specify how a network service is *identified*.

We find that Nagayama's watermark filter identifies a watermark value in a file in network traffic and matches that value to a filtering rule that is *active* for the associated source and destination addresses. Ex. 1003 ¶ 33. Nagayama also filters network traffic with a firewall using addresses and a network service protocol of the traffic to enable traffic to a watermark filter. *Id.* ¶¶ 37, 38. Because the watermark filter applies its filter rules only to network traffic sent by network services that a firewall enables, the rules are *active* for those network services. *Id.* Petitioner adds network services to Nagayama's database of filter rules to filter traffic further by *addresses and watermark value for a particular network service(s)*. Pet. 38–39.

We agree with Petitioner that it would have been obvious to amend Nagayama's database of filter rules to specify the network service protocols for which each filter rule is active, and Crawford describes how to do this for a firewall so that it would have been obvious to apply this known technique to Nagayama's similar filter rules for predictable results within the level of ordinary skill in the art. *See* Pet. 18–23, 28–39; *KSR*, 550 U.S. at 416, 417.

Claims 1 and 11 do not recite, nor does the '282 patent describe, how network traffic "is associated with a particular network service." Ex. 1001, 16:42–46, 17:56–60. Petitioner contends that Nagayama and Crawford use a firewall to identify network protocols, which can be done using well-known port numbers that indicate each protocol, and by inspecting data packets to identify network services. Pet. 18–23, 28–39; Reply 27–28. Dr. Mohapatra testifies that Nagayama and Crawford filter traffic based on its associated network service (Ex. 1002 ¶ 96), and firewalls filter packets based on well-known port numbers for network services in packet headers (*id.* ¶ 120). We agree with these contentions, and we credit Dr. Mohapatra's testimony.

Notably, claims 1 and 11 do not require the network security device or a watermark filter to *identify* a network service associated with traffic. Nor is Petitioner *burdening* Nagayama's watermark filter with identifying the network service that is associated with traffic as Patent Owner asserts. *See* PO Resp. 45; PO Sur-reply 6; Pet. 18–23, 28–39.

As claimed, the network security device *identifies* a watermark value. Then, it *determines* if a filtering rule exists with that value and is active for the associated network service. The evidence does not show that a look up operation in a table of filter rules is unpredictable or beyond the level of skill in the art. We find that Nagayama uses a look up table of watermark values with source and destination addresses and action fields. Adding a field for network services associated with the traffic is just one more field. Pet. 38. Once a watermark value is identified, finding a filter rule that is active for the network service can be performed the same way the value is matched to source and destination addresses with no further modification or complexity or time-consuming analysis required. Ex. 1003 ¶¶ 23–28, 32–38, Figs. 2, 3.

The '282 patent describes watermark detection module 210 analyzing a file for a watermark value. This value is compared with rules in a filter database to determine if a match exists. Ex. 1001, 14:8–27. This description indicates a skilled artisan can implement this function predictably. The '282 patent describes gateway 104 as a network security device with firewall module 208 that could identify network services for watermark detection module 210 to use with its DLP rules to filter traffic by rules active for those services. *Id.* at 6:40–7:47. Claims 1 and 12 do not specify how network traffic is "associated with a particular network service." The "wherein" clause simply recites attributes of the network traffic. *Id.* at 16:43–46.

"The reasonable expectation of success requirement refers to the likelihood of success in combining references to meet the limitations of the claimed invention." *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016) ("[F]ailure to consider the appropriate scope of the . . . patent's *claimed invention* in evaluating the reasonable expectation of success . . . constitutes a legal error that [is] review[ed] without deference.") (citation omitted); *see Elekta*, 81 F.4th at 1376 (holding that a finding of a reasonable expectation of success can be implicit and can be based on the arguments and evidence presented and considered, including the motivation to combine).

Petitioner has shown by a preponderance of the evidence that a skilled artisan would have had a reasonable expectation of success in modifying Nagayama's filtering means 60 and filtering rules to add network services so each filter rule specifies watermark values, addresses, *and* network services for which the rule is active to filter network traffic. Support is shown in the prior art references and knowledge in the art as discussed *supra* and below.

Petitioner asserts, and Patent Owner does not dispute, that Nagayama and Crawford teach a skilled artisan how to maintain databases with filtering rules that comprise fields for watermark values, addresses, actions, *and network services* as claimed. Pet. 18–22 (citing Ex. 1003 ¶¶ 21, 24–29, 32–35, 37, 38, Figs. 1, 2; Ex. 1004, 8:13–25, Fig. 5), 26–39 (citing Ex. 1003 ¶¶ 19, 24, 26–28, 32, 34, 37, 38, Fig. 2; Ex. 1004, 2:24–28, 2:48–51, 7:46–47, 9:10–13, Fig. 5; Ex. 1009, 6 ("database" definition)). We agree.

Figure 2 of Nagayama depicts storage means 63 as a table that stores filter rules for external transfer conditions used by filtering means 60 to enable or disable external data transfers. Ex. 1003 ¶¶ 20, 23–29, 33.

Crawford stores firewall policies and parameters used by firewall 101 to filter network data in database 110 implemented in any suitable database system. Ex. 1004, 6:29–45, 7:8–19. Configurations for filtering rules are stored in database 110 in tabular form with different settings for different network protocols. *Id.* at 7:8–60, 8:9–29. *Active rules* are organized by application and protocol settings. *Id.* at 8:13–16, 9:1–16, Figs. 4–8.

We find that the teachings of Nagayama and Crawford evidence a predictability in maintaining a database of filter rules of watermark values and network services for which the filter rules are active so a skilled artisan would have had a reasonable expectation of success in creating a "filter database containing a plurality of filtering rules," as claimed, based on their teachings. Ex. 1003 ¶¶ 23–29, Fig. 2; Ex. 1004, 6:29–7:19, 8:4–12, Fig. 5.

The '282 patent evidences predictability in creating a database of filter rules. Ex. 1001, 11:26–57 (filter rules for watermarks can be stored in a database and *other fields can be added or removed* to the rules). The '282 patent offers no guidance for creating a database of filter rules stating only, "watermark detection module 210 includes a package of DLP rules" used to search traffic passing through gateway 104 for patterns. *Id.* at 7:39–43.

Petitioner asserts, and Patent Owner does not dispute, that Nagayama uses a network security device to determine whether a watermark filtering rule matches a watermark value embedded in a file and the watermark filter rule is *active* for a particular source and destination (domain/host name), and Crawford determines by a network security device whether a database of filtering rules has an *active* filter rule for a particular source and destination and network service as claimed. Pet. 45–48 (citing Ex. 1003 ¶¶ 23–27, 33, 37, 38, Figs. 2, 3; Ex. 1004, 9:18–27, Fig. 9); Ex. 1002 ¶¶ 88–93. We agree.

Dr. Mohapatra testifies that Nagayama and Crawford improve content filtering systems for data sent over an open network, and their overlapping objectives and technologies complement one another to improve filtering. Ex. 1002 ¶ 95. Dr. Mohapatra also testifies that Nagayama's system "could be improved by including content-based filtering on a network service into a single policy" with all parameters in a single rule. *Id.* ¶ 96. Dr. Mohapatra testifies that Nagayama and Crawford filter traffic for network services and skilled artisans filter data at gateways for network services and watermarks using port numbers and packets. *Id.* ¶¶ 49, 54–61, 64–66, 70–73, 119–127. His testimony supports Petitioner's assertion that skilled artisans would have combined Nagayama and Crawford to add network services to a database of filter rules with a reasonable expectation of success. Pet. 22–23, 35–37.

Dr. Black testifies a skilled artisan would not have had a reasonable expectation of success in modifying Nagayama's watermark filtering means 60 to filter network traffic for network services or apply filter rules that are active for a network service due to the complexity of firewall systems and design challenges. Ex. 2001 ¶ 45. This testimony is not credible because claims 1 and 11 do not claim a firewall or a network security device with any of the complex features or functions that Dr. Black describes.

Dr. Black testifies that firewalls support address and port ranges in syntax and filtering steps and packet queue interfaces. Ex. 2001 ¶ 45. His testimony is consistent with that of Dr. Mohapatra, who testifies, "network services are associated with well-known port numbers and the filtering at the gateways can be based on these well-known port numbers." Ex. 1002 ¶ 120 (firewalls screen packets using port numbers identified in packet headers). Thus, identifying network services is well-known and predictably done.

We determine that Petitioner has demonstrated by a preponderance of evidence that a skilled artisan would have had a reasonable expectation of success in modifying Nagayama's database of watermark filtering rules to add network services for which those rules are active as claimed.

k. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1 and 11 are unpatentable over Nagayama and Crawford.

5. *Claims 2 and 12*

Claims 2 and 12 depend, respectively, from claims 1 and 11 and recite that the action includes one or more of (i) logging information associated with observation of the file, (ii) blocking the file, (iii) quarantining a user associated with the file, (iv) quarantining an Internet Protocol (IP) address of a sender of the file, and (v) quarantining an interface of the network security device through which the file was received. Ex. 1001, 16:58–64, 18:9–16.

a. Petitioner's contentions

Petitioner contends that Nagayama discloses the action of blocking the data from being transmitted to the receiving device when the result of the determination indicates the transfer is disabled as shown by Transfer Rule 3 that blocks (disables transfer of) traffic that matches its filter policy. Pet. 50–51 (citing Ex. 1003 ¶¶ 11, 27, Fig. 2). Petitioner contends that Crawford discloses quarantining content and using a list of spam addresses and logging information whenever particular traffic was identified. *Id.* at 51 (citing Ex. 1004, 1:56–58, 5:38–41, claim 23; Ex. 1002 ¶¶ 157–159).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding claims 2 and 12. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 2 and 12 are unpatentable over Nagayama and Crawford.

E. Ground 2: Alleged Obviousness Over Nagayama, Crawford, and Hawthorn

Petitioner contends that claims 1, 2, 11, and 12 are unpatentable under 35 U.S.C. § 103(a) over Nagayama, Crawford, and Hawthorn. Pet. 51–52.

1. Hawthorn

Hawthorn relates to information security and identification of network vulnerabilities resulting from interconnection of public and private networks that exposes networks to risk of attacks such as data exfiltration that causes unauthorized release of data from a computer system or network. Ex. 1005 ¶¶ 1, 2, 4. Hawthorn teaches that data exfiltration can occur with third-party Web-based services like DropBox and Webmail such as Gmail. *Id.* ¶ 24.

2. Petitioner's contentions

Petitioner contends that a skilled artisan would have been motivated to incorporate well-known network services like DropBox, which is a data synchronization service, and Gmail, which is a Web-based email network service, into the Nagayama-Crawford combination to increase the number of services for which traffic is monitored and improve the flexibility and scope of content that is monitored for such popular applications to protect users and networks. Pet. 51–52 (citing Ex. 1005 ¶ 24; Ex. 1002 ¶¶ 160–162).

3. Patent Owner's arguments

Patent Owner argues that Petitioner does not rely on Hawthorn's teachings to support its proposal to add these services to Nagayama and Crawford. PO Resp. 41. Patent Owner argues that Petitioner does not show that Dropbox or Gmail had specific security vulnerabilities that would have motivated a skilled artisan to detect and filter data communications using those services for watermark bearing files. *Id.* at 42. Patent Owner asserts that filtering traffic for viruses and spam involves incoming traffic whereas Nagayama's watermark filtering means 60 filters *outgoing* data to prevent data leakage, and watermark filtering would not identify those threats. *Id.* at 42–43.

4. Analysis

An obviousness "analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court to take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR*, 550 U.S. at 418. "[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its application is beyond his or her skill." *Id.* at 417. A person of ordinary skill is a person of ordinary creativity who is able to "fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 420–21. We agree with Petitioner's contentions that a skilled artisan would have used the watermark/DLP technique of Nagayama and Crawford to filter popular network services such as Dropbox and Gmail that are used to transfer data between networks and need to be monitored for data leakage like other network services, as Hawthorn teaches. Pet. 51–52; Reply 25.

We find that Hawthorn teaches such popular Web-based services must be inspected for security vulnerabilities that could result in *data exfiltration*. Ex. 1005 ¶¶ 24, 25. The issue is not whether these services are more or less vulnerable than other network services filtered by the Nagayama-Crawford combination. The issue is that these popular services are used to transfer data between networks such that a skilled artisan would have been motivated to protect against data leakage from an enterprise by enterprise users of such network services by including these network services in the watermark filtering system of Nagayama and Crawford for similar benefits of improved security, flexibility, and granularity. Dr. Mohapatra testifies that including these network services in the Nagayama-Crawford combination "would have improved the number of services for which traffic could be monitored – thereby strengthening the filtering systems from a safety standpoint" and "would have improved the flexibility, scalability, and scope of content monitoring." Ex. 1002 ¶ 161. We find that Hawthorn's teachings and Dr. Mohapatra's testimony credibly support Petitioner's reasons for making the combination. Petitioner's reasoning is supported by record evidence and therefore is not conclusory. Nor does Patent Owner address these rationales or their underpinnings sufficiently to undermine Petitioner's obviousness rationales and contentions in Ground 2. PO Resp. 42.

5. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 1, 2, 11, and 12 are unpatentable over Nagayama, Crawford, and Hawthorn.

F. Ground 3: Alleged Obviousness Over Nagayama, Crawford, and Sharma

Petitioner asserts claims 3, 5–8, 13, and 15–18 are unpatentable under 35 U.S.C. § 103(a) over Nagayama, Crawford, and Sharma. Pet. 52–62.

1. Sharma

Sharma describes a system and method for encrypting a watermark payload by applying a hash function and embedding the hash value in an object like a document. Ex. 1006 ¶¶ 148, 149, Abstr., Fig. 8. The system generates a hash of a payload and communicates the hash to a watermark embedder that embeds the hash in an object like a document or electronic file. *Id.* ¶ 148. A watermark decoder can analyze the document to recover the hash value and payload information from the data repository. *Id.* ¶ 149.

2. Motivation to Combine and Expectation of Success

a. Petitioner's contentions

Petitioner asserts that a skilled artisan would have combined Sharma's watermark content filtering and message securing with content filtering of Nagayama and Crawford to improve content filtering, watermark capability, security, and efficiency by preventing tampering, storing more information in a watermark, and providing a fast, efficient way to retrieve data. Pet. 53–54 (citing Pet. § VII.A.; Ex. 1006 ¶¶ 148, 149; Ex. 1002 ¶¶ 163–166).

Petitioner asserts that Sharma uses a hash function that produces a standardized bit-length hash regardless of the input payload size, and this standardization would allow watermark payloads of different lengths to be embedded as a fixed-length watermark in documents to make detection and decoding of the watermark more reliable and easier to perform. Pet. 54 (citing Ex. 1006 ¶¶ 148, 167; Ex. 1002 ¶ 167).

Petitioner contends that a skilled artisan would have been able to combine Sharma's content filtering techniques with the complementary content filtering techniques of Nagayama and Crawford with a reasonable expectation of success because applying a hash function to a watermark payload combines hash functions that have been known for decades and applied widely to watermarks as a combination of known prior art elements to yield predictable results. Pet. 53–54 (citing Ex. 1002 ¶ 168).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions that it would have been obvious to combine Sharma with Nagayama and Crawford with a reasonable expectation of success. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine Petitioner has shown, by a preponderance of the evidence, that it would have been obvious to combine Sharma's watermark content filtering and hashing with Nagayama and Crawford with a reasonable expectation of success.

3. Claims 3 and 13

a. Petitioner's contentions

Petitioner asserts that Sharma discloses applying a hash function to a watermark payload as a data repository receiving a watermark payload and generating a corresponding hash of the payload, and Nagayama discloses a watermark payload may include information specific to a user or company associated with the file and a sensitivity level of the file so applying a hash function to such a watermark payload would include information specifying a company and sensitivity associated with the file and sensitivity level. Pet. 55 (citing contentions for elements 1[a][ii]/11[a][ii]; Ex. 1006 ¶¶ 57, 148).

Regarding "a watermark payload including . . . information specifying a user with which the file is associated," Petitioner contends that Sharma discloses payload message bits that can define a numeric owner field, an image/item field, a plurality of fields, and private portions linked to sensitive information of a person's medical record, social security number, name, birth date, and a driver's license number. Pet. 55–56 (citing Ex. 1006 ¶¶ 57, 101, 136, 141, 148; Ex. 1002 ¶¶ 169–172). Petitioner asserts that Nagayama discloses to embed data on the internal network with information identifying the data such as an electronic watermark with information indicative of the copyright, confidentiality, and like of the data. *Id.* at 56 (citing Ex. 1003 ¶ 19). Petitioner asserts that it would have been obvious to have included such information in watermarks to specify a user with which the file is associated to improve the ability to track, monitor, and control data using user-specific information that would allow a specific user's content to be prohibited from external transfer or require biometric information to identify a particular user and prevent other users from transferring or receiving the user-specific data. Pet. 56–57 (Ex. 1002 ¶¶ 169–172).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding the unpatentability of claims 3 and 13 over Nagayama, Crawford, and Sharma. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 3 and 13 are unpatentable over Nagayama, Crawford, and Sharma.

4. Claims 5 and 15

a. Petitioner's contentions

Petitioner contends that converting the result of a hash function or a message-digest algorithm to Base-64 encoding as recited in claims 5 and 15 was widely known and disclosed in the 2009 edition of the Dictionary of Computer and Internet Terms (CIT) indicating Base-64 encoding was widely known and within a skilled artisan's knowledge. Pet. 57 (citing Ex. 1009, 3 (definition of "Base-64")). Petitioner asserts a skilled artisan would have converted the hash function to Base-64 encoding to improve the system's flexibility by encoding data into printable ASCII characters to allow data to be sent via email systems. *Id.* (citing Ex. 1009, 3; Ex. 1002 ¶¶ 173–174).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding the unpatentability of claims 5 and 15 over Nagayama, Crawford, and Sharma. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 5 and 15 are unpatentable over Nagayama, Crawford, and Sharma.

5. Claims 6 and 16

a. Petitioner's contentions

Petitioner contends that Sharma and Nagayama use a client program to embed a watermark value in a file to be protected as in claims 6 and 16, and the '282 patent describes a "client" as an application program, process, or device in a client/server relationship such that it can be a program on the client side. Pet. 57–58 (citing Ex. 1001, 4:27–30; Ex. 1002 ¶ 175).

Petitioner contends that Nagayama's electronic watermark addition means 31 added an electronic watermark to *data to be transmitted* and thus that needs to be protected, and a skilled artisan would have found it obvious that this means was a separate client program as Nagayama demarcates it with a separate box as part of a client device that embeds watermarks into data prior to the data being received by the filtering means. Pet. 58–59 (citing Ex. 1003 ¶ 21, Fig. 1; Ex. 1002 ¶¶ 176–177).

Petitioner asserts that Sharma discloses a watermark embedder and explained that the hash was communicated to a watermark embedder that embedded the hash in an object like a document or an electronic file and is depicted as a separate element that would be obvious to be a separate client program. Pet. 59–60 (citing Ex. 1006 ¶ 148, Fig. 8; Ex. 1002 ¶ 178).

b. Patent Owner's arguments

Patent Owner argues that Petitioner focuses on whether a separate client program performs the embedding but does not address whether the watermark value is embedded/inserted into a file "responsive to the file being identified as one that is to be protected" as recited in claims 6 and 16. PO Resp. 66. Patent Owner asserts "[t]here is no analysis on whether or how the prior art ***identifies*** a file as one that is to be protected and then, ***responsive*** to that identification, proceeds with embedding/inserting the watermark into the file." *Id.* at 67. Patent Owner argues that Nagayama's disclosure of adding a watermark "to data to be transmitted" "says nothing about whether or how Nagayama's electronic watermark addition means *identifies* files to which watermarks need to be added before it adds the watermark." *Id.* ("That the data will be transmitted is irrelevant to the issue of file identification.").

Patent Owner asserts that Petitioner's contentions for Sharma fail for the same reason because communicating a hash to a watermark embedder that embeds the hash into a document "says nothing about whether or how Sharma identifies files to which watermarks need to be added before it adds the watermark." PO Resp. 67 ("That the watermark is communicated to the embedder is irrelevant to the issue of file identification.").

c. Analysis

We agree with Petitioner that Nagayama teaches to identify files to be watermarked. The '282 patent describes a watermarking program installed on a computer system "to mark a target set of files/documents in the network 100 with a watermark." Ex. 1001, 6:4–7. A user runs a watermarking program on a server containing a target set of files to be protected, and configures the list of files to be marked, sets the watermark to be used, and applies it to the list of files. *Id.* at 6:18–23. No details are provided for how a "target set of files" is identified by the user, the enterprise, or an entity.

Nagayama discloses that "data transmission device 30 has data to be transmitted to another information processing device, and adds electronic watermark information to the transmission data in accordance with rules defined for the data." Ex. 1003 ¶ 21. A file is identified as one that is to be protected *based on rules defined for the data*. *Id.* The rules identify files to be watermarked like a target set of files to be protected in the '282 patent. Ex. 1001, 6:4–7. Nagayama's electronic watermark addition means 31 adds an electronic watermark to *data to be transmitted*. Pet. 58 (citing Ex. 1003 ¶ 21). We find that a file is identified as one to be watermark/protected when it is to be transmitted, and it meets a filter rule. Reply 29 ("Otherwise, watermarks would be added to documents that do not need one.").

We disagree with Dr. Black's testimony that Nagayama does not *identify* files that need watermarks (Ex. 2004 ¶ 116) because he does not address Nagayama's teaching of data transmission device 30 (and watermark addition means 31) adding electronic watermarks to data *in accordance with rules defined for the data* (Ex. 1003 ¶ 21 (emphasis added)). Watermarks are added to data that is to be transmitted according to rules that define data to be protected and confidentiality. Ex. 1003 ¶¶ 19, 21; *see* Pet. 58–59.

In Sharma, a payload that is desired to be protected is communicated to a data repository that stores the payload, generates a hash of the payload, and communicates the hash to a watermark embedder, "which embeds the hash in an object like a document or electronic file." Ex. 1006 ¶ 148. Thus, Sharma has a target list of payloads that are hashed and sent to a watermark embedder, which embeds the hash in a document or file to be protected. *Id.* We find that Sharma identifies files and documents to be protected and uses a watermark embedder to embed a hash in such objects as claimed. *Id.*

d. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 6 and 16 are unpatentable over Nagayama, Crawford, and Sharma.

6. Claims 7, 8, 17, and 18

a. Petitioner's contentions

Petitioner contends that Sharma uses watermarks with sensitive data such as a person's medical records or social security number, and it would have been obvious to include a command-line client program in Sharma's watermark embedder to improve security by allowing such private data to be entered manually rather than stored or received over a network. Pet. 60–61.

Petitioner asserts that command-line programs were known by 2012, used in Unix systems as identified by the '282 patent, and defined in the 2009 edition of the Dictionary of CIT. Petitioner asserts that using such programs to embed watermarks would have improved the Nagayama-Crawford system by embedding watermarks via inexpensive, readily-available command-line client programs that were standard in nearly every operating system. Pet. 61 (citing Ex. 1009, 5 (definition of "command line" and "command prompt"), 9 (definition of "Unix"), 12 (definition of "Linux"); Ex. 1001, 6:9–10; Ex. 1002 ¶¶ 179–181). Petitioner asserts that including a file directory, file name, or the sensitivity level of the data in the watermark as claimed would add criteria by which data could be filtered and indicate a sensitivity level to make the system more capable of identifying and acting on sensitive information. *Id.* at 61–62 (citing Pet. § VIII.C.2.; Ex. 1002 ¶ 182).

b. Patent Owner's arguments

Patent Owner argues that a skilled artisan would have understood that sensitive information still can be stored locally or received over a network, and a command-line program does not impact on that issue. PO Resp. 68. Patent Owner argues that it would have been impractical or impossible for the administrator who enters such information manually into a command-line program to memorize such information of different individuals instead of having it stored and then entering it using the command-line program. *Id.* at 68–69. Patent Owner argues that such programs need to be programmed to perform the claimed functions, and Petitioner does not address "why specifically those programs would be used versus other means to perform the claimed functions." *Id.* at 69.

c. Analysis

The '282 patent describes the use of a command line client program to insert watermarks into documents to customize watermarks that are inserted into documents. Ex. 1001, 8:65–10:40. We find persuasive Petitioner's contentions that using such programs in Nagayama-Crawford-Sharma would have allowed similar customized entry of sensitive and other data consistent with the description of this process in the '282 patent. Pet. 60–62. This rationale is consistent with Petitioner's reasons for combining teachings of Nagayama and Crawford for claims 1 and 11, from which claims 7, 8, 17, and 18 depend, to improve the security, efficiency, and granularity of DLP systems and prevent leakage by enabling customization and consideration of other filtering factors such as network services and watermark values for increased sensitivity, identity, and granularity that improve DLP filtering. Pet. 22–23, 29–39; Reply 2–5. We agree that customizing DLP by using a command-line program would improve the DLP, security, and granularity of Nagayama and Crawford similarly and such programs are relatively inexpensive and available on operating systems. Pet. 61–62; *see also KSR*, 550 U.S. at 417 ("[I]f "a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.").

d. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 7, 8, 17, and 18 are unpatentable over Nagayama, Crawford, and Sharma.

G. Ground 4: Alleged Obviousness Over Nagayama, Crawford, Sharma, and Wolge

Petitioner contends that claims 4 and 14 are unpatentable under 35 U.S.C. § 103(a) over Nagayama, Crawford, Sharma, and Wolge. Pet. 62.

1. Wolge

Wolge describes the use of hashing algorithms to generate identifiers. Ex. 1007 ¶¶ 87–89. Wolge discloses hashing algorithms are optimized for different purposes, and a Fowler/Noll/Vo (FNV) algorithm is optimized for fast processing efficiency while maintaining a low collision rate. *Id.* ¶ 89.

2. Petitioner's contentions

Petitioner asserts that Wolge discloses hashing an identifier using hashing algorithms that include FNV algorithms (Fowler/Noll/Vo), and Petitioner contends that the FNV algorithm was well-known and frequently used for this function. Pet. 62 (citing Ex. 1007 ¶ 89; Ex. 1002 ¶ 183). Petitioner asserts that a skilled artisan would have applied an FNV algorithm to a watermark to create a unique identifier because it was efficient and designed to be fast while maintaining a very low collision rate. *Id.*

3. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding the unpatentability of claims 4 and 14 over Nagayama, Crawford, Sharma, and Wolge. *See generally* PO Resp.; Sur-reply.

4. Analysis

The '282 patent describes running an FNV hash on a watermark so it can be inserted in a document and searched by the gateway. Ex. 1001, 9:15–24. Wolge describes a similar use of the FNV algorithm to generate unique searchable identifiers. Ex. 1007 ¶¶ 2, 8, 87–89; *see KSR*, 550 U.S. at 417.

5. Conclusion

Based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of the evidence, that claims 4 and 14 are unpatentable over Nagayama, Crawford, Sharma, and Wolge.

H. Ground 5: Alleged Obviousness over Jones and Crawford

Petitioner contends that claims 1, 2, 11, and 12 are unpatentable under 35 U.S.C. § 103(a) over Jones and Crawford. Pet. 62–84.

1. Jones

Jones filters watermarks in network traffic to prevent dissemination of confidential information to unauthorized recipients. Ex. 1008, Abstr., 1:11–62, 2:31–46. Network traffic can be emails sent by an email server and data sent by FTP and Web servers. *Id.* at 1:63–2:15, 4:55–57, Fig. 3. Watermark detection and reading program (WDRP) 1305 detects watermarks and takes actions specified in watermark filter rules for different user and recipient groups specified in a table, which is reproduced below. *Id.* at 3:61–4:10.

Sender Group	Recipient Group	Flag Conditions	Action
S1	R1	011	Send message
S1	R2	110	Do not sent message notify the administrator
S1	R2	001	Send message, and log fact that S1 sent a message to R2.
S1	R2	101	Return message to sender
S2	R1	011	Send message
S2	R3	110	Do not sent message and notify the system administrator

Logic rules in the table are implemented in database 401 with watermark flag conditions and actions. *Id.* at 3:47–4:15. A message from Sender S1 is sent to Recipient R1 if a Flag Condition is 011. *Id.* A message is not sent from Sender S1 to Recipient R2 if a Flag Condition is 110. *Id.* Figure 3 of Jones is reproduced below to illustrate an email system implementation.

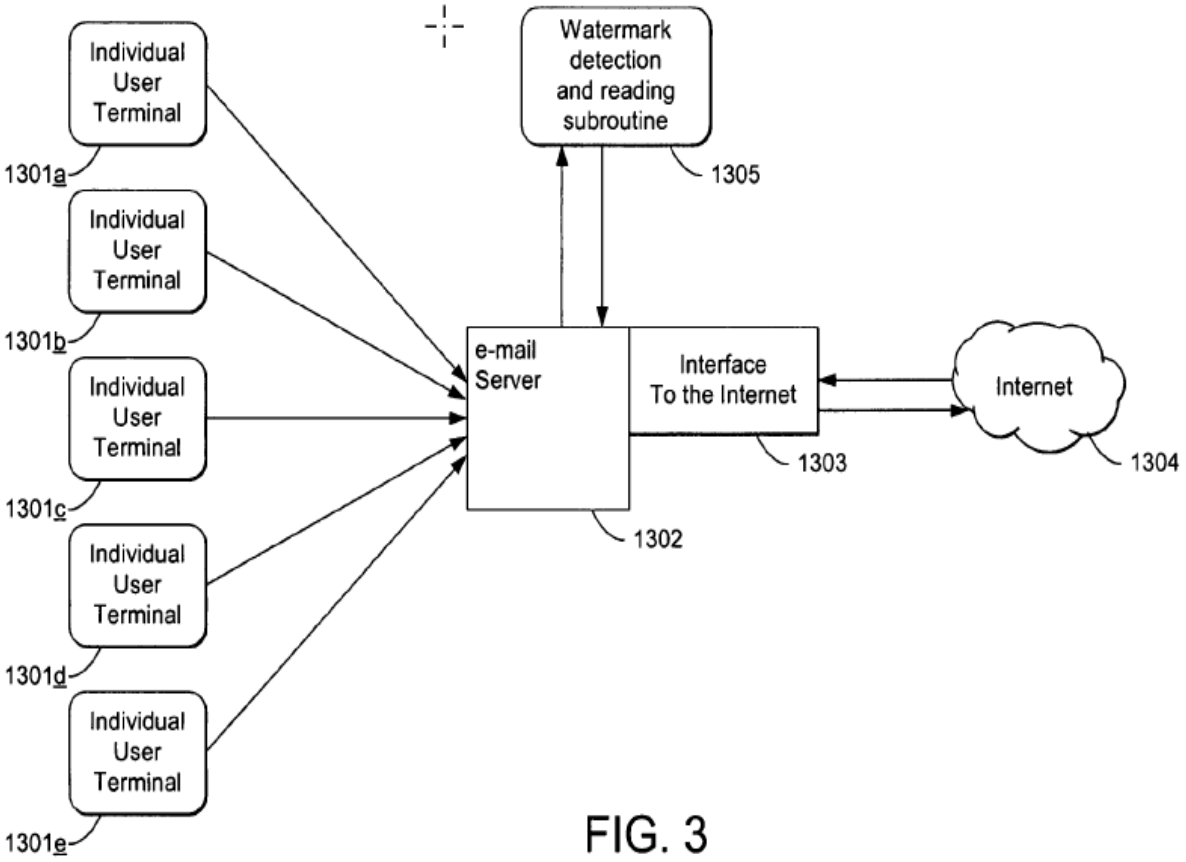


FIG. 3

Figure 3 above depicts an email system with user terminals 1301 connected to email server 1302, which interfaces 1303 to Internet 1304. Before server 1302 transmits a message from a user terminal to Internet 1304, the message and attached documents are passed through WDRP 1305, which determines if the message contains a watermark, detects flag bits contained therein, and takes action specified in the filter rules. *Id.* at 3:21–4:48. WDRP 1305 can filter documents on Web and FTP servers and take actions. *Id.* at 2:13–17.

2. Motivation to Combine and Expectation of Success

a. Petitioner's contentions

Petitioner contends that a skilled artisan would have been motivated to combine the complementary techniques of Jones and Crawford to improve their content filtering of documents sent over networks such as the Internet. Pet. 65. Petitioner asserts that a skilled artisan would have combined Jones' use of digital watermarks to control document transmission with Crawford's content filtering policies for network services to improve content filtering. *Id.* (citing Ex. 1008, 1:41–43; Ex. 1004, Abstr.; Ex. 1002 ¶ 187).

Petitioner asserts that combining the teachings of Jones and Crawford would have improved the flexibility, security, and convenience of content filtering. Petitioner asserts that Jones filters email content based on sender, recipient, and watermark payload and teaches that this filtering technique can be applied to FTP and Web servers and *include more rules* depending on the application. Pet. 65–66 (citing Ex. 1008, 2:31–49, 4:14–17, 4:55–57). Petitioner contends that a skilled artisan would have considered Crawford's teachings, which allow a user to filter traffic according to policies specific to the network service associated with traffic, because Jones would have been improved by adding the ability to control policies for a variety of network services from a single policy database. *Id.* at 66 (citing Ex. 1004, 2:21–32). Petitioner asserts that this capability would have enabled Jones' system to structure filtering policies according to particular characteristics and vulnerabilities of particular network services to improve security thereby. *Id.* (citing Ex. 1002 ¶ 188). Petitioner contends that filtering content based on a network service would have been obvious to try when a limited number of criteria can be used to filter traffic. *Id.* at 67 (citing Ex. 1002 ¶ 188).

Petitioner asserts that a skilled artisan would have found it obvious to filter by network services in Jones because Jones' system is used with Email, FTP, and Web servers, and Jones discloses that its filter rules can contain as many rules as are needed for a particular application such that it would have been obvious to filter traffic sent by email, FTP, and Web servers in a single system and specify the network services for which each rule applied. *Id.* at 73–74 (citing Ex. 1008, 4:14–17, 4:55–57; Ex. 1002 ¶¶ 203, 204). Petitioner asserts that Crawford and Jones already filter network traffic by source and destination so including network services of the traffic in the rules of Jones would have addressed the well-known fact that network services have more than one application and/or protocol for network communications and email such that a skilled artisan would have found it obvious to provide filtering rules that filter traffic based on multiple network services/protocols to avoid blind spots in the system. *Id.* at 75–76 (citing Ex. 1002 ¶¶ 205–209).

b. Patent Owner's arguments

Patent Owner argues that Petitioner's "contention that 'Jones did not describe how policies could be managed ***once the system was expanded to control email, Web, and FTP content'*** . . . incorrectly presumes Jones teaches or suggests a multi-server computer network that includes three servers: email, FTP, and Web. It does not." PO Resp. 47. Patent Owner argues that Petitioner's assertion that a skilled artisan would have modified Jones based on Crawford's teachings to control policies for a variety of network services from a single policy database is "founded on a falsehood" because "[t]here is simply no multi-server network having a plurality of policy databases disclosed in Jones for Petitioner to coalesce into [a] single policy database." *Id.* at 48.

Patent Owner asserts that Petitioner does not explain what a multi-server network would look like in Jones, and Petitioner provides no details regarding how Jones' email, FTP, and Web servers would be arranged relative to one another, to network devices in the local network, and to interfaces to external networks including the Internet. PO Resp. 48–49.

c. Analysis

As discussed below, we are persuaded by Petitioner's assertions and evidence that this subject matter is unpatentable over Jones and Crawford.

i. Jones' email server embodiment

We find that a skilled artisan would have combined Crawford's teaching of a database of filtering rules that are active for multiple network services and protocols with Jones' email server to filter emails sent by different network service *protocols* with different security concerns and vulnerabilities to improve the security, flexibility, and granularity of Jones. Pet. 65–66, 75–76; Dec. Inst. 47. Crawford teaches that email uses different network protocols such as SMTP, IMAP, and POP3, and each network service can have different filter rules for greater granularity and security. Ex. 1004, 7:29–8:3, 9:1–16, Fig. 4 (multiple settings provided for SMTP 403, IMAP 404, POP3 405), Fig. 7 (customized settings for SMTP 704, IMAP 705, POP3 706), Fig. 8 (email protocols 802 include SMTP, IMAP, POP3 network protocols that can have different settings). Crawford's rules database is configurable with different filter rules that are *active for different email network service protocols* such as SMTP, IMAP, and POP3 and "not all configuration settings are appropriate for all protocols" so other settings and parameters may be configured. *Id.* at 7:29–8:3. Crawford's techniques would have improved Jones' email filtering similarly. *KSR*, 550 U.S. at 417.

Jones discloses that its database 401 of filter rules (in § III.H.1. *supra*) "is merely a simplified example of the rules and combinations that could be in database 401 [and] [t]he database could include hundreds or thousands of users and it could include dozens of rules." Ex. 1008, 4:13–16.

ii. Jones' WDRP works with Web and FTP servers

Jones discloses that "[t]he system can be complex or simple as desired for a particular application." Ex. 1008, 4:16–18. Jones further discloses that "similar precautions [as its email system embodiments] could be taken with FTP servers or with Web servers." *Id.* at 4:55–57. This disclosure supports Petitioner's proposal to use Jones' WDRP with email, Web, and FTP servers to protect confidential data sent by those servers. *Id.* at 1:17–2:17, 4:55–57; Ex. 1004, 1:6–2:10 (security policies set by an administrator); Pet. 65–67.

We agree with Petitioner that Jones *and* Crawford describe a network of email, FTP, and Web servers, and Crawford's database of filter rules for email, Web, and FTP network services would have improved Jones' ability "to efficiently control policies for multiple network services" because "[b]eing able to filter content based on a network service would have improved the operation of Jones' system by adding the ability to control policies for a variety of network services from a single policy database." Pet. 66; *id.* at 73–76. We find that Jones' email server connects senders and recipients via different email applications and *protocols* (e.g., POP3, SMTP, IMAP) with different vulnerabilities so Crawford's filtering would improve security, flexibility, and granularity of Jones' email server 1302 to control data traffic between senders and recipients on upstream and downstream connections. Pet. 66, 73–76; Ex. 1004, 1:6–2:10, 7:20–60, 9:1–40, Figs. 7, 8 (802); Ex. 1002 ¶¶ 117, 203, 207, 208; Ex. 1008, 3:21–4:38; Dec. Inst. 47.

Crawford's database of filter rules for email (SMTP, IMAP, POP3), Web (HTTP), and FTP is shown in Figures 7 and 8, reproduced below.

Config Name	703 HTTP Service	704 SMTP Service	705 IMAP Service	706 POP3 Service	707 FTP Service	708 Options
701 Strict	Banned Word [x] Url Block [x] AV Scan [x] File Block [x] . . .	AV Scan [x] File Block [x] Frag Email [ ] Pass [ ] Spam block [x] . . .	AV Scan [x] File Block [x] Frag Email [ ] Pass [ ] Spam block [x] . . .	AV Scan [x] File Block [x] Frag Email [ ] Pass [ ] Spam block [x] . . .	AV Scan [x] File Block [x] . . .	Modify, Delete
702 Scan	Banned Word [x] Url Block [x] AV Scan [x] File Block [ ] . . .	AV Scan [x] File Block [ ] Frag Email [ ] Pass [ ] Spam block [ ] . . .	AV Scan [x] File Block [ ] Frag Email [ ] Pass [ ] Spam block [ ] . . .	AV Scan [x] File Block [ ] Frag Email [ ] Pass [ ] Spam block [ ] . . .	AV Scan [x] File Block [ ] . . .	Modify, Delete
. . .						
None						

Figure 7

Figure 7 above shows rules for email services of SMTP, IMAP, and POP3, Web services of HTTP, and FTP as does Figure 8 below. Ex. 1004, 9:1–7.

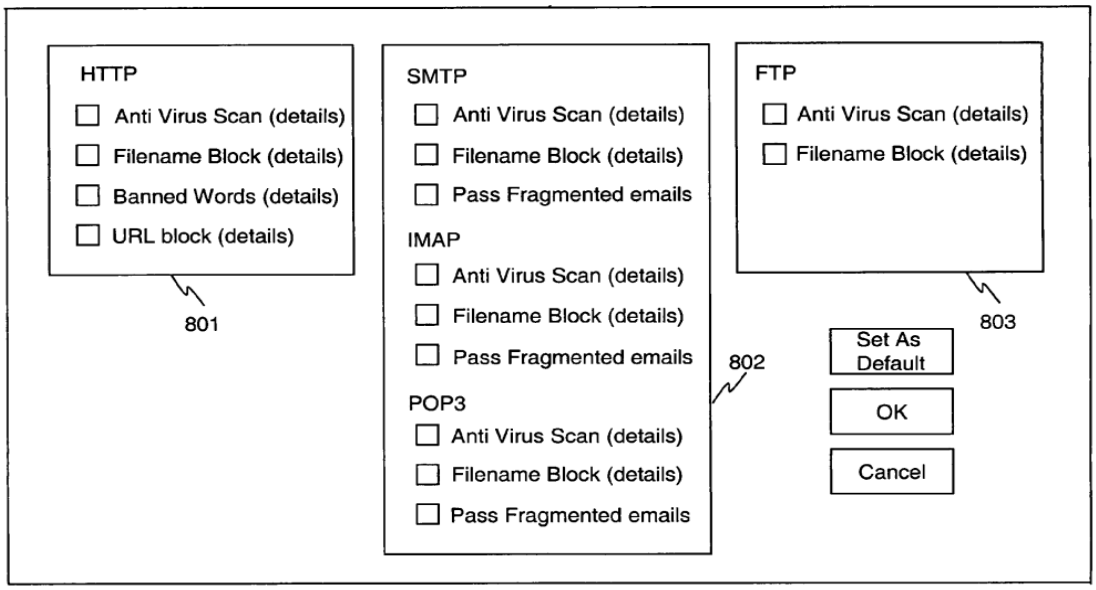


Figure 8

Figure 8 depicts filter rules that can be *active* for *web protocol 801* (HTTP), *email protocols 802* (SMTP, IMAP, POP3), and *file transfer protocol 803* (FTP) and that could be used in Jones. Ex. 1004, 9:8–15. Users customize filter settings for each network service shown in Figure 4 reproduced below.

Scheme 4

Options	401 HTTP	402 FTP	403 SMTP	404 IMAP	405 POP3	406 SMB/CIFS	407
Antivirus Scan	□	□	□	□	□	□	
Filename Block	□	□	□	□	□	□	
Quarantine	□	□	□	□	□	□	
Banned Word	□		□	□	□		408 △
Spam Block			□	□	□		
URL Block	□						409 △
URL Exempt	□						410 △
Option A	□	□	□	□	□	□	
Option B	□	□	□	□	□	□	
Option C	□	□	□	□	□	□	
. . .	. . .	. . .	. . .	. . .	. . .	. . .	

Figure 4

Figure 4 shows filter rule configurations for email service protocols SMTP, IMAP, and POP3, Web service HTTP 401, and FTP 402. Ex. 1004, 7:29–35. "Any other suitable protocols may be used." *Id.* at 7:36–37.

A skilled artisan would have combined Jones' teachings of databases of watermark filter rules for email, FTP, and Web services with Crawford's teaching of a single database of filter rules for all these protocols. *KSR*, 550 U.S. at 421. Jones at the least suggests a system of email, Web, and FTP servers, and Crawford shows that such multi-server systems were known in the art and configured with active filter rules *in a single database* as claimed. Ex. 1008, 1:63–2:56, 4:44–47; Ex. 1004, 7:20–8:29, 9:1–16.

Jones expressly discloses that its invention addresses "security challenges to corporations" presented by the Internet and to others with computers that store confidential information with connections to the Internet. Ex. 1008, 1:17–19. Jones expressly discloses the applicability of its system for email, the Web, and FTP servers and applications by disclosing an embodiment for email and by additionally disclosing that

> [m]essages and documents also enter the Internet and other electronic networks from servers such as Web servers and FTP servers. In a similar fashion a watermark detection program can interrogate documents on servers such as Web and FTP servers and take action as described above.

Ex. 1008, 2:13–17.

We find that Jones uses its watermark detection program with email, Web, and FTP servers, because security precautions must be taken for each by a corporation. Ex. 1008, 2:13–17, 4:55–57. Jones and Crawford teach that these network services and protocols can be integrated for a corporation to improve its network security more flexibly and granularly. *Id.* at 4:55–57; Ex. 1004, 1:11–45. A skilled artisan could have combined these teachings like pieces of a puzzle and would have done so for enterprises that conduct business over the Internet or other network using these network service protocols. *KSR*, 550 U.S. at 420–21. Even if multiple servers are used to handle multiple protocols, a single database 110 would store filter rules for all the servers (and their WDRP(s)) as Crawford teaches to do for multiple network protocols for flexibility and granularity. Ex. 1004, 6:3–45, 7:8–8:3, Figs. 4, 5, 7, 8. Crawford teaches how to configure email, Web, and FTP servers in a multi-server network like Jones teaches/suggests using *a single database 110 of filter rules* for all network services. *Id.*; *cf.* PO Resp. 48.

Crawford configures firewalls as hosts running proxy servers for each network service, but Crawford configures a *single database of filter rules* for all of the proxy servers and network services as a preferred way to filter efficiently. Ex. 1004, 4:43–67, 6:3–45, 7:29–8:29, 9:1–16, Figs. 1, 4–8.

Jones configures a WDRP on email server 1302 and provides a single database 401 of rules for the watermark detector 1305. Ex. 1008, 3:21–4:34, Figs. 3, 4. Whether each email, Web, and FTP server in Jones is configured with WDRPs, as Patent Owner asserts (PO Resp. 53–54), Crawford teaches that such proxy-like WDRPs use a *consolidated database of filter rules* for email (e.g., SMTP, IMAP, POP3), Web (HTTP), and FTP servers. *See* Ex. 1004, 4:43–67, 6:3–45, 7:8–8:29, 9:1–16, Figs. 1, 4–8; Dec. Inst. 46.

We find that Crawford improves security using filter rules for source and destination address, network protocols, and other parameters in a *single filter rule* stored in a *single database* used for filtering multiple protocols and applications, Jones recognizes the need to filter email, Web, and FTP network applications for corporate security, and Crawford teaches how to do that for Web, email, and FTP to improve Jones' ability to filter email, Web, and FTP traffic. Ex. 1008, 2:13–17, 4:55–57; Ex. 1004, 4:43–67, 6:3–45, 7:8–8:29, 9:1–16, Figs. 1, 4–8; *see In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) (a determination of obviousness based on teachings of multiple references does not require actual, physical substitution of the elements).

d. Conclusion

We determine that Petitioner has established, by a preponderance of the evidence, that a skilled artisan would have been motivated to combine the teachings of Jones and Crawford to render claims 1 and 11 unpatentable with a reasonable expectation of success.

3. Claims 1 and 11

a. 1[pre]/11[pre]

i. Petitioner's contentions

Petitioner asserts that Jones discloses a method for protecting against data leaks using a network security device to protect an enterprise network as watermark detection and reading program (WDRP) 1305 to inspect traffic passing from a local area network to the external Internet. Pet. 67–69 (citing Ex. 1008, 1:17–19, 1:22–25, 1:41–43, 2:33–39, 3:25–28, 3:32–4:10, Abstr., claims 1–4; Ex. 1002 ¶¶ 190–195; Ex. 1001, 5:10–14).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding elements 1[pre]/11[pre]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Regardless of whether the preamble is limiting, based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of evidence, that Jones and Crawford disclose or suggest elements 1[pre]/11[pre].

b. 1[a][i]/11[a][i]

i. Petitioner's contentions

Petitioner asserts that Jones protected a local area (enterprise) network with a watermark detection routine program that maintained a database of transfer rules and logic to implement the rules. Pet. 69–71 (citing Ex. 1008, 3:48–58, 3:60–4:11 (table), Figs. 3, 4; Ex. 1002 ¶¶ 196–198).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding elements 1[a][i]/11[a][i]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of evidence, that Jones and Crawford disclose or suggest elements 1[a][i]/11[a][i].

c. 1[a][ii]/11[a][ii]

i. Petitioner's contentions

Petitioner asserts that Jones' transfer rules specify a watermark value as Flag Conditions, owner, and confidentiality with an action to take by the watermark filter program such as sending or not sending a message for network services that included email, Web services, and FTP that a skilled artisan would understand include various protocols. Petitioner contends that Jones teaches that its filter rules database can contain as many rules as are needed for a particular application and could apply to email, FTP, and Web servers, and a skilled artisan would have combined them into a single system with a single policy database to increase the scope and efficiency of the system and avoid blind spots that could occur if the system only filtered for one email protocol. Pet. 71–74 (citing Ex. 1008, 3:60–4:17 (table), 4:55–57, Fig. 2; Ex. 1002 ¶¶ 199–204). Petitioner also contends that Crawford teaches filter rules for multiple network services, and a single rule applies to multiple network services such as "Any" services and a rule for email could apply to applications like Gmail and Yahoo Mail and protocols like IMAP, SMTP, and POP3 and could be grouped by type as Crawford recognized to avoid blind spots in the system. *Id.* at 74–76 (citing Ex. 1004, 2:24–28, 2:48–51, 7:46–47, 9:10–13, Figs. 5, 6; Ex. 1002 ¶¶ 199–209).

Petitioner also illustrates a policy database that combines Jones and Crawford, and we reproduce that policy database below.

Jones and Crawford Combined

Sender	Recipient	Flag Conditions	Network Service	Action
S1	R1	011	HTTP	Send message
S1	R2	110	FTP	Do not sent message notify the administrator
S1	R2	001	Email, POP3, SMTP	Send message, and log fact that S1 sent a message to R2.
S1	R2	101	Dropbox, Gmail	Return message to sender
S2	R1	011	FTP, HTTP	Send message
S2	R3	110	FTP, HTTP, Gmail, Dropbox	Do not sent message and notify the system administrator

The table above illustrates a filter rule policy database that combines Jones' and Crawford's respective teachings by Petitioner's contentions. Pet. 76.

ii. Patent Owner's arguments

Patent Owner argues that Jones discloses a database of filter rules for its email server but does not disclose how to structure databases for Web and FTP servers, and Petitioner's proposed policy database makes little sense for HTTP and Web servers that do not send messages/documents between users as email servers do but instead store uploaded documents until a request is received from potential users. PO Resp. 49–51. Patent Owner argues that "Petitioner's proposed modified filter database above erroneously includes fields, such as 'sender" and 'recipient,' for FTP and Web servers." *Id.* at 51. Patent Owner argues that the proposed modification of a single database has no benefit because a hypothetical multi-server system in Jones already can take *different* actions for a given file sent by each server. *Id.* at 53–55. Patent Owner asserts that Dr. Mohapatra's testimony that a single database would apply uniform rules to different protocols to prevent leaks contradicts the need to address security vulnerabilities of each protocol. *Id.* at 55–57.

iii. *Analysis*

As discussed in § III.H.2.c. *supra*, we find that Crawford combines filter rules for different network services in a single database to provide greater flexibility for an administrator to configure parameters to filter and process various network content without compromising network security. Ex. 1004, 1:56–2:32, 6:3–45, 7:8–8:3, Figs. 4–8. A single database of rules provides more granular control and flexibility over settings by using a *set of rules* to handle all of the passing network traffic or any specific portion thereof. *Id.* at 4:7–23. Crawford's system intercepts data packets sent by POP3, SMTP, IMAP, HTTP, and FTP and can provide a filter setting(s) for each protocol, and Crawford teaches that not all configuration settings are appropriate for all protocols. *Id.* at 6:3–16, 7:29–60, 9:1–16, Figs. 4, 7, 8.

We find that Crawford applies rules to traffic sent by *FTP* between a *source and destination*, which contradicts Patent Owner's arguments that traffic cannot be sent between a source and destination by FTP. Ex. 1004, 8:13–29, Figs. 5, 6. A Web server that sends email using HTTP can be controlled by filter rules that also consider *source and destinations* (*id.*) as Dr. Mohapatra testifies (PO Resp. 56 (quoting Ex. 2003, 56:16–57:18)).

We find that a database of filter rules applicable to multiple network services would eliminate blind spots that could occur if a security system only filtered some email protocols and not others, and data leaks could occur by users of non-filtered network services as Dr. Mohapatra testifies. *See* Ex. 1002 ¶¶ 205–209. Dr. Mohapatra testifies this could occur for example for Web-based email if a system/filter database only filtered SMTP, IMAP, and/or POP3 network service protocols for email and did not provide filter rules for a server that handled Web-based email. Ex. 2003, 56:16–57:18.

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[a][ii]/11[a][ii].

d. 1[a][iii]/11[a][iii]

i. Petitioner's contentions

Petitioner asserts that Crawford discloses network services recited in elements 1[a][iii]/11[a][iii] so a skilled artisan would have found it obvious to filter Web-based email based on Crawford's teachings of email services and HTTP and device synchronization services based on teaching of P2P, HTTP, FTP, and IMAP that can be used for device synchronization. Pet. 76–78 (citing Ex. 1004, 1:38–40, 6:3–16, 7:46–47; Ex. 1009, 4 (definition of "BitTorrent" file sharing service), 8 (definition of "IMAP"); Ex. 1005 ¶ 24; Ex. 1011, 3 (definition of "iCloud"); Ex. 1002 ¶¶ 210–214).

ii. Patent Owner's arguments

Patent Owner again argues that the analysis for element 1[a][iii] is divorced from arguments concerning motivations to combine for element 1[a][ii] for the same reasons as Ground 1. PO Resp. 63.

iii. Analysis

As discussed in § III.D.4.d.ii *supra*, some protocols have more secure versions, which supports Petitioner's reasons to filter vulnerable versions, with the other reasons provided by Petitioner for the combination.

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[a][iii]/11[a][iii].

e. 1[b][i], 1[b][ii]/11[b][i], 11[b][ii]

i. Petitioner's contentions

Petitioner contends that Jones uses a watermark filter to protect a local area (enterprise) network by receiving traffic originated in that network and directed to the Internet outside the network with a file, and both Jones and Crawford disclose and suggest that the traffic is associated with a network service such as email, Web servers, and FTP and with various networking protocols. Pet. 78–79 (citing Ex. 1004, 6:3–5, 9:32–37; Ex. 1008, 2:15–17, 2:53–55, 3:27–29. 3:32–38, claim 3, Fig. 3; Ex. 1002 ¶¶ 216–218).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding elements 1[b][1], 1[b][ii], 11[b][i], and 11[b][ii]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[b][1], 1[b][ii], 11[b][i], and 11[b][ii].

f. 1[c]/11[c]

i. Petitioner's contentions

Petitioner asserts that Jones' watermark filter (watermark detection and reading program 305) identifies a watermark embedded in received data and determines flag values included as part of the watermark to determine if a specific action should be taken. Pet. 79–80 (citing Ex. 1008, 3:38–41, 3:49–4:11 (table), Fig. 2; Ex. 1002 ¶ 219).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions for regarding elements 1[c] and 11[c]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[c] and 11[c].

g. 1[d]/11[d]

i. Petitioner's contentions

Petitioner contends that Jones' watermark filter determines whether a detected watermark value matches a watermark value specified in a transfer rule and determines an action to take for a particular message based on the flag settings in the watermark payload, and a skilled artisan would have found it obvious to determine whether the rule was active for a particular network service based on Crawford's teachings to use the protocol to identify an associated firewall policy. Pet. 80–82 (citing Ex. 1008, 3:12–20, 4:31–34, claim 7, Fig. 2; Ex. 1004, 9:18–27, Fig. 9; Ex. 1002 ¶¶ 219–223).

ii. Patent Owner's arguments

Patent Owner asserts the same arguments for elements 1[d]/11[d] as were asserted for elements 1[a][ii]/11[a][ii]. PO Resp. 49–63.

iii. Analysis

We disagree with Patent Owner's arguments for the reasons discussed in § III.H.3.c. *supra*. Moreover, we find that the '282 patent provides no description of what is meant by a filtering rule being *active* for a particular network service, other than it is applied by the watermark filter to certain network services and not to others. *See* Ex. 1001, 1:62–2:21, Abstr.

We find that Jones discloses a watermark filter that applies filtering rules that are "active" for a particular service because the rules are applied to files sent by that network service containing watermark values that match a value in the table, and Jones discloses a database of filter rules that are active for particular network services such as email service. We find that Crawford discloses a filtering database that applies rules to network service protocols for which the rules are active because traffic sent by certain network service protocols is filtered by rules that are active for the protocols. Configurations of filtering rules are stored in database 110 in tabular form with different settings for different network protocols. Ex. 1004, 7:8–60, 8:9–29. The rules in Crawford's database of filter rules are organized by network service application and network service protocol settings for which each rule is *active*. *Id.* at 8:13–16, 9:1–16, Figs. 4–8.

iv. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[d] and 11[d].

h. 1[e]/11[e]

i. Petitioner's contentions

Petitioner contends that Jones discloses the watermark filter taking an action specified by a transfer rule when the traffic matches the transfer rule. Pet. 82–83 (citing Ex. 1008, 4:31–34; Ex. 1002 ¶¶ 224–225).

ii. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions for regarding elements 1[e] and 11[e]. *See generally* PO Resp.; Sur-reply.

iii. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that Jones and Crawford disclose or suggest elements 1[e] and 11[e].

i. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of evidence, that claims 1 and 11 are unpatentable over Jones and Crawford.

4. Claims 2 and 12

a. Petitioner's contentions

Petitioner contends that Jones discloses transfer rules that can specify an action to take if the traffic conditions match a policy, and the action may include blocking a data transfer and logging and sending a message, and Crawford discloses actions that include quarantining content and logging when particular traffic is identified. Pet. 83–84 (citing Ex. 1008, 3:60–4:10 (table); Ex. 1004, 1:56–58, 5:38–41, claim 23; Ex. 1002 ¶¶ 226–227).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's contentions regarding claims 2 and 12. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 2 and 12 are unpatentable over Jones and Crawford.

I. Ground 6: Alleged Obviousness over Jones, Crawford, and Hawthorn

Petitioner contends that claims 1, 2, 11, and 12 are unpatentable under 35 U.S.C. § 103(a) over Jones, Crawford, and Hawthorn. Pet. 84–85.

1. Petitioner's contentions

Petitioner contends, to the extent Crawford does not disclose Web-based email and a device synchronization for elements 1[a][iii]/11[a][iii], Hawthorn discloses network services such as DropBox that provides data synchronization and Gmail that is Web-based email. Pet. 84–85 (citing Ex. 1005 ¶ 24). Petitioner asserts that a skilled artisan would have found it obvious to add these network services to the Jones-Crawford combination to monitor more network services and improve the flexibility and scope of the content monitoring because Gmail and DropBox are well-known, popular applications likely used by numerous users. Pet. 85 (citing Ex. 1002 ¶¶ 228, 229). Petitioner asserts that extending traffic monitoring operations to such popular applications would help to protect individual users and their networks. *Id.*

2. Patent Owner's contentions

Patent Owner raises similar arguments as for Ground 2. PO Resp. 41–43, 63–66. Patent Owner argues that Petitioner relies on a single paragraph in Hawthorn to allege that DropBox and Gmail are "well-known network services," but Petitioner does not rely on Hawthorn's teachings to support its contentions that a skilled artisan would have found it obvious to add these services to the Jones-Crawford combination. PO Resp. 64. Patent Owner asserts that Petitioner has not shown that Gmail and DropBox have security vulnerabilities or should be filtered for watermark bearing files. *Id.*

Patent Owner argues that protecting against computer viruses and spam protects an enterprise network from *incoming* data communications rather than *outgoing* data and has nothing to do with preventing leakage of confidential data. PO Resp. 64–65. Patent Owner asserts that modifying Jones' filter rules to filter data based on watermark values and general use of Gmail or DropBox communications does not filter out viruses, spam, and malware with any level of specificity. *Id.* at 65.

3. Analysis

For the reasons discussed for Ground 2 *supra*, Petitioner's reasons to modify the Jones-Crawford combination to filter Dropbox and Gmail are supported by rational underpinnings based on Hawthorn's teachings that DropBox and Gmail are well-known network services that must be inspected for security vulnerabilities that can result in *data exfiltration* (Ex. 1005 ¶¶ 1, 2, 4, 24, 25), and the services are used widely as Dr. Mohapatra testifies (Ex. 1002 ¶ 229) such that a skilled artisan would have been motivated to include these network services in the filter rules of Jones and Crawford to improve network security, flexibility, and granularity (Pet. 85). *See DyStar*, 464 F.3d at 1368. Hawthorn focuses on security and network vulnerability including *data exfiltration* and discloses the need to monitor and filter third-party network services such as DropBox and Gmail for data exfiltration (Ex. 1005 ¶¶ 1, 2, 4, 23–25) that would benefit the watermark filtering techniques of Jones and Crawford similarly for improved security and granularity.

4. Conclusion

Based on the parties' contentions and record evidence, we determine Petitioner has demonstrated, by a preponderance of the evidence, that claims 1, 2, 11, and 12 are unpatentable over Jones, Crawford, and Hawthorn.

J. Ground 7: Alleged Obviousness Over Jones, Crawford, and Sharma

Petitioner contends that claims 3, 5–8, 13, and 15–18 are unpatentable under 35 U.S.C. § 103(a) over Jones, Crawford, and Sharma. Pet. 85–92.

1. Motivation to combine

Petitioner contends that a skilled artisan would have been motivated to combine Sharma with Jones and Crawford because Sharma used improved means to secure messages for content filtering that was complementary to, and would have improved, the content filtering of Jones and Crawford to include the watermark capabilities to prevent data leakage. Petitioner asserts that Sharma's disclosure of applying a hash function to a watermark payload would have provided several well-known benefits to Jones and Crawford to include preventing tampering, allowing storage of more information in the watermark, and providing a fast, efficient way to retrieve data compared to other data structures to improve security and efficiency. Pet. 85–86 (citing Pet. §§ VIII.E., VIII.E.1. for Ground 5; Ex. 1006 ¶¶ 148, 149, Abstr.; Ex. 1002 ¶¶ 231–233). Petitioner contends that using Sharma's hash function would allow watermark payloads of different lengths to be embedded as fixed-length watermarks so watermark detection and decoding would be easier and more reliable. *Id.* at 86 (citing Ex. 1006 ¶ 148; Ex. 1002 ¶ 234).

Patent Owner does not contest Petitioner's assertions regarding the motivation to combine Sharma with Jones and Crawford. *See generally* PO Resp.; Sur-reply.

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that it would have been obvious to combine Sharma with Jones and Crawford.

2. Reasonable expectation of success

Petitioner contends that a skilled artisan would have been motivated to combine Sharma with Jones and Crawford with a reasonable expectation of success because all three references concerned improved means for securing messages by content filtering, Sharma's content filtering techniques were complementary with Jones and Crawford and provided well-known benefits, and the combination merely combined well-known, widely used prior art elements of hash functions to yield predictable results. Pet. 85–87 (citing Pet. §§ VIII.E., VIII.E.1. for Ground 5; Ex. 1002 ¶¶ 231–235).

Patent Owner does not contest Petitioner's assertions regarding the reasonable expectation of success in combining Sharma with Jones and Crawford. *See generally* PO Resp.; Sur-reply.

Based on the parties' contentions and record evidence, we determine Petitioner has established, by a preponderance of the evidence, that a skilled artisan would combine Jones, Crawford, and Sharma with a reasonable expectation of success to render obvious claims 3, 5–8, 13, and 15–18.

3. Claims 3 and 13

a. Petitioner's contentions

Petitioner contends that Sharma discloses applying a hash function to a watermark payload that includes a variety of different information, and Jones discloses watermark payloads with company information as discussed for elements 1[a][ii]/11[a][ii] and recited in claims 3 and 13, and it would have been obvious to add user information such as social security number, name, and driver's license number to improve the ability to track, monitor, and control data. Pet. 87–88 (citing Ex. 1005 ¶¶ 57, 101, 136, 141, 148; Ex. 1008, 3:13–15; Ex. 1002 ¶¶ 236–239).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding claims 3 and 13. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 3 and 13 are unpatentable over Jones, Crawford, and Sharma.

4. Claims 5 and 15

a. Petitioner's contentions

Petitioner contends that Base-64 coding was widely known by the priority date of the '282 patent as shown by the 2009 edition of the CIT Dictionary, and a skilled artisan would have converted the hash function to Base-64 encoding to improve the system's flexibility by encoding data into printable ASCII characters to allow data to be sent through email systems that handle text. Pet. 89 (citing Ex. 1009, 3 (definition of "Base 64"); Ex. 1002 ¶¶ 240, 241).

b. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding claims 5 and 15. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 5 and 15 are unpatentable over Jones, Crawford, and Sharma.

5. Claims 6 and 16

a. Petitioner's contentions

Petitioner contends that Sharma uses a separate client program to embed a watermark value into a file to be protected like the '282 patent's use of a client application, program, process, or device in client-server relationship, and a hash is communicated to a separate client watermark embedder that embeds the hash in a document or electronic file. Pet. 89–90 (citing Ex. 1006 ¶ 148; Ex. 1001, 4:27–30; Ex. 1002 ¶¶ 242, 243).

b. *Patent Owner's arguments*

Patent Owner argues that Petitioner focuses on the client program that embeds the hash but "[t]here is no analysis on whether or how the prior art ***identifies*** a file as one that is to be protected." PO Resp. 66–67.

c. Analysis

As discussed in § III.F.5 *supra*, the '282 patent describes a watermark program that may "mark a target set of files/documents in the network 100 with a watermark." Ex. 1001, 6:4–7. A user runs a watermark program on a server containing a target set of files to be protected, configures the list of files to be marked, sets the watermark, and applies it to files. *Id.* at 6:18–23.

In Sharma, a payload that is desired to be protected is communicated to a data repository that stores the payload, generates a hash of the payload, and communicates the hash to a watermark embedder, "which embeds the hash in an object like a document or electronic file." Ex. 1006 ¶ 148. Thus, Sharma has a target list of payloads used to generate hashes that are sent to a watermark embedder, which embeds the hash in a document or file that is to be protected. *Id.* We find that Sharma identifies files/documents to protect and embeds a hash in such objects with a watermark embedder. *Id.*

d. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 6 and 16 are unpatentable over Jones, Crawford, and Sharma.

6. Claims 7, 8, 17, and 18

a. Petitioner's contentions

Petitioner contends that Sharma's watermark embedder could include sensitive private personal information in a watermark, and it would have been obvious that Sharma's watermark embedder could include a command-line client program to improve system security by entering such private data manually because such programs were well known by 2012 and include file directory information to indicate if a file was sensitive. Pet. 90–92 (citing Ex. 1006 ¶ 101; Ex. 1009, 5, 9, 12; Ex. 1001, 6:9–10; Ex. 1002 ¶¶ 244–246).

b. Patent Owner's arguments

Patent Owner argues that sensitive information can be stored locally or received over a network and entered manually so that a command-line program does not impact whether the information is stored locally and an administrator could not memorize this information before entering it into a command-line program. PO Resp. 68–69. Patent Owner asserts that the Petition does not address why these programs would be used. *Id.* at 69.

c. Analysis

The '282 patent describes an embodiment that uses a command line client program to insert watermarks into documents. Ex. 1001, 8:65–66. The description indicates that such programs permit customization of the watermarks inserted into documents. *Id.* at 8:65–10:40.

We find that Petitioner's contentions that such programs customize entry of sensitive data in Jones-Crawford-Sharma is consistent with the '282 patent (Pet. 60–61) and is consistent with Petitioner's reasons to combine teachings of Jones and Crawford for claims 1 and 11, from which claims 7, 8, 17, and 18 depend, to improve the security and the efficiency and granularity of DLP to prevent leakage by the customizing and considering other filtering factors such as network service and watermark values/data sensitivity and identity. Implementing this customization using a command-line program would improve DLP filtering, security, and granularity and would be available on most operating systems. Pet. 91–92; *see KSR*, 550 U.S. at 417 (the use of a known technique used to improve one device to improve similar devices in the same way is obvious unless its application is beyond the level of ordinary skill in the art).

d. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 7, 8, 17, and 18 are unpatentable over Jones, Crawford, and Sharma.

K. Ground 8: Alleged Obviousness Over Jones, Crawford, Sharma, and Wolge

Petitioner asserts that claims 4 and 14 are unpatentable under 35 U.S.C. § 103(a) over Jones, Crawford, Sharma, and Wolge. Pet. 92.

1. Petitioner's contentions

Petitioner contends that it would have been obvious to use a Fowler-Noll-Vo algorithm to hash a watermark, as Wolge teaches, because it was "designed to be fast while generally maintaining a very low collision rate" as Wolge teaches. Pet. 92 (citing Ex. 1002 ¶ 248).

2. Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions regarding claims 4 and 14. *See generally* PO Resp.; Sur-reply.

3. Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated, by a preponderance of the evidence, that claims 4 and 14 are unpatentable over Jones, Crawford, Sharma, and Wolge.

IV. CONCLUSION

Petitioner has shown by a preponderance of evidence that claims 1–8 and 11–18 of the '282 patent are unpatentable.

Claims	35 U.S.C. §	References/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 2, 11, 12	103(a)	Nagayama, Crawford	1, 2, 11, 12	
1, 2, 11, 12	103(a)	Nagayama, Crawford, Hawthorn	1, 2, 11, 12	
3, 5–8, 13, 15–18	103(a)	Nagayama, Crawford, Sharma	3, 5–8, 13, 15–18	
4, 14	103(a)	Nagayama, Crawford, Sharma, Wolge	4, 14	
1, 2, 11, 12	103(a)	Jones, Crawford	1, 2, 11, 12	
1, 2, 11, 12	103(a)	Jones, Crawford, Hawthorn	1, 2, 11, 12	
3, 5–8, 13, 15–18	103(a)	Jones, Crawford, Sharma	3, 5–8, 13, 15–18	
4, 14	103(a)	Jones, Crawford, Sharma, Wolge	4, 14	
Overall Outcome			1–8, 11–18	

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–8 and 11–18 of the '282 patent have been shown to be unpatentable; and

FURTHER ORDERED that because this is 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.[8]

[8] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding, 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. 16654 (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).

PETITIONER:

Thomas Millikan
Babak Tehranchi
PERKINS COIE LLP
millikan-ptab@perkinscoie.com
tehranchi-ptab@perkinscoie.com

PATENT OWNER:

James M. Glass
John T. McKee
Quincy Lu
Andrew M. Holmes
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com