



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,920	03/09/2004	Kenneth L. Levy	P0951	3347
23735	7590	01/31/2013	EXAMINER	
DIGIMARC CORPORATION			CORBO, NICHOLAS T	
9405 SW GEMINI DRIVE			ART UNIT	PAPER NUMBER
BEAVERTON, OR 97008			2427	
			MAIL DATE	DELIVERY MODE
			01/31/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KENNETH L. LEVY

Appeal 2010-007767
Application 10/797,920
Technology Center 2400

Before DAVID M. KOHUT, JASON V. MORGAN, and
BRYAN F. MOORE, *Administrative Patent Judges*.

MORGAN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Introduction

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1, 4, 7 – 11, 13 – 18, and 25 – 31. Claims 2, 3, 5, 6, 12, and 19 – 24 are cancelled. We have jurisdiction under 35 U.S.C. § 6(b)(1).

We affirm.

Invention

The invention is directed to adding intelligence information to the headers of internet protocol (IP) packets, thus enabling a firewall to determine if a given packet, without requiring other packets from the same content and without touching the data within the given packet, can be forwarded. *See Abstract.*

Exemplary Claims (Emphases Added)

1. A method of enforcing geographical restrictions on content redistribution in a TCP/IP [transmission control protocol/internet protocol] network in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts:

defining a geographical boundary across which certain content data does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and

determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more single-bit flags included in the header data of said packet;

wherein said one or more flag bits are related to the payload of a watermark in the content data.

4. A method of *providing entertainment content from a distributor to a home*, while governing potential redistribution of the content from the home, the method including forming an IP packet having header data and body data, wherein the body data includes content data, and the header data includes a first destination address within the home to which the distributor intends the content data be delivered, the method comprising:

the distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating:

(a) it is not permissible to send a copy of the content data in the packet to any second destination address; or

(b) it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and

wherein said domain comprises networked devices associated with a single family, and restriction on potential redistribution of the content is defined by reference to the intended first address.

7. The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and *the additional data includes a field signaling that copying of data in said packet to said second destination address should be:*

(a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location.

8. The method of claim 7 *wherein the first and second destination addresses are within a common domain.*

25. A method of deterring unauthorized redistribution of video entertainment from a consumer's home network, the consumer's home network employing at least a computing device and a networking device;

wherein acts performed by the computing device include:

ascertaining restriction information for the video entertainment, said ascertaining including at least one of: (a) extracting restriction information from header data conveyed with the video entertainment; (b) obtaining restriction information from a remote repository associated with the video entertainment; or (c) *discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment;*

dividing the video entertainment among payload portions of plural IP packets;

including data indicating said ascertained restriction information in header portions of each of said IP packets; and

sending the packets to the networking device;

and wherein acts performed by the networking device comprise examining said included data and *refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network.*

26. The method of claim 25 *wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment.*

27. The method of claim 25 wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment.

28. The method of claim 25 *wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.*

Rejections

The Examiner rejects claims 4, 7 – 9, 11, and 13 – 17 under 35 U.S.C. § 102(e) as being anticipated by Roese (US 2003/0217122 A1; Nov. 20, 2003). Ans. 3 – 7.

The Examiner rejects claims 1, 10, 18, 25, 26, and 28 under 35 U.S.C. § 103(a) as being unpatentable over Roese and Levy '899 (US 2001/0044899 A1; Nov. 22, 2001). Ans. 8 – 12.

The Examiner rejects claim 27 under 35 U.S.C. § 103(a) as being unpatentable over Roese, Levy '899 and Levy '844 (US 2002/0186844 A1; Dec. 12, 2002). Ans. 12 – 13.

The Examiner rejects claims 29 – 31 under 35 U.S.C. § 103(a) as being unpatentable over Roese, Levy '899, and Medvinsky (US 2005/0071663 A1; Mar. 31, 2005; filed Sept. 26, 2003). Ans. 13 – 14.

ISSUE 1

With respect to claim 4, Appellant argues that the arrangement of Roese “inserts a tag in certain packets. This tag indicates that the packets should not be accessed if found outside a specified location (e.g., outside a particular campus, etc.). [This] tag thus has only a single state [indicating] a single type of restriction.” App. Br. 10. Appellant further

argues “[t]he restriction in Roese is not defined by reference to the intended first address,” App. Br. 12, and that “Roese does not teach limiting distribution of content data to a *second* destination address as a function of the *first* destination address,” Reply Br. 2.

Issue

Did the Examiner err in finding that Roese discloses a “distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating: (a) it is not permissible to send a copy of the content data in the packet to any second destination address; or (b) it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and wherein . . . restriction on potential redistribution of the content is defined by reference to the intended first address,” as recited in claim 4?

Analysis

The Examiner finds that Roese, which is directed to location-based access control in a data network, discloses the disputed recitations because Roese discloses a tag used for generating a packet with additional data for placing transmission restrictions with defined boundaries such as a present device, a room, a campus, etc. *See* Ans. 4 – 5 (citing, e.g., Roese ¶¶ [0115] – [0117] and fig. 6). In particular, the Examiner finds that the different defined boundaries correspond to additional data multiple states, where (1) the

restriction to a “present device” discloses that “it is not permissible to send a copy of the content data in the packet to any second destination address” and (2) the restriction of a “room,” “building,” “campus,” etc. discloses that “it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address.” *See* Ans. 4 and 16. The Examiner finds that these restrictions on the potential redistribution of the content are defined by reference to the intended first address (i.e., either to a particular device or to a domain that includes a particular device). *See* Ans. 5.

We agree with the Examiner that Roesse’s tag, by providing for different levels of copying restrictions, discloses at least two different states. We agree with the Examiner’s finding that the restriction to a “present device” restricts packet content data from being copied to a second destination address (i.e., to a device having a second destination address). Further, the Examiner correctly finds that the other disclosed restrictions of Roesse, such as a “room,” “building,” or “campus,” represent expanding domains, encompassing the “present device.” *See* Ans. 16. Thus, we agree with the Examiner that these other disclosed restrictions restrict packet content data to second destination addresses within a domain that also includes the first destination address (i.e., that encompasses the “present device”). We also agree with the Examiner that, since the restrictions are defined with respect to a “present device” or to a domain that encompasses the “present device,” the restriction on potential redistribution of content is defined by reference to an intended first address (i.e., the address of the “present device”). Therefore, we agree with the Examiner that Roesse

discloses “distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of the content data in the packet to a second destination address different than the first destination address, wherein the additional data has at least two states, respectively indicating: (a) it is not permissible to send a copy of the content data in the packet to any second destination address; or (b) it is not permissible to send a copy of the content data in the packet to any second destination address except to a second destination address within a domain that also includes the first destination address; and wherein . . . restriction on potential redistribution of the content is defined by reference to the intended first address,” as recited in claim 4.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 4, and dependent claims 7 – 10 and 30, with respect to this issue. Appellant makes similar arguments with respect to claim 11. App. Br. 16. For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 11, and dependent claims 13 – 18 and 31, with respect to this issue.

ISSUE 2

Appellant argues that an interpretation of claim 4 “that somehow makes the user in the home also the claimed ‘distributor’ is too tortured to be sustained.” App. Br. 11.

Issue

Did the Examiner err in finding that Roesse discloses claim 4's preamble recitation of a "method of providing entertainment content from a distributor to a home"?

Analysis

The Examiner correctly finds that:

the role of the distributor is not defined by the claim language to occur at a location that is necessarily separate from the home. No supported reasoning is provided by the Appellant as to why the user at the home is entirely incapable of forming packet header data with the additional data. Nothing in the art would be understood by a person having ordinary skill in the art that would prevent a user in conjunction with the use of a computer at the home from creating packet headers from typical interactions with the Internet.

Ans. 17; *see also* Fin. Rej. 2.

We agree with the Examiner that the claim recitations do not preclude the distributor from being within the home to which content is distributed. Moreover, preamble recitations generally do not limit the claims unless the recitations recite essential structure or steps, or unless the recitations are necessary to give life, meaning, and vitality to the claims. *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010). The disputed recitation does not affect the steps of the claimed invention (i.e., "the distributor forming said header data to additionally include additional data . . .") and is not necessary to give meaning to the claim. Thus, even though we agree with the Examiner that the limitation is disclosed by the reference, Appellant cannot show error in the Examiner's rejection by arguing that

Roese fails to disclose claim 4's preamble recitation of a "method of providing entertainment content from a distributor to a home."

Accordingly, we do not find Appellant's arguments persuasive of error in the Examiner's rejection of claim 4, and dependent claims 7 – 10 and 30, with respect to this issue.

ISSUE 3

Appellant argues that "claim 4 specifies that the domain comprises networked devices 'associated with a single family.' Again, Roese has no such teaching." App. Br. 12.

Issue

Did the Examiner err in finding that Roese discloses "wherein said domain comprises networked devices associated with a single family," as recited in claim 4?

Analysis

The Examiner finds that Roese, by disclosing that "exchanging the content may be limited to within the domain of [a] single family such as any network devices within a campus," discloses a domain that comprises networked devices associated with a single family. *See* Ans. 5. The Examiner also finds that the Specification does not "define 'family' to have any meaning other than a common definition." *See* Ans. 17. As such, we agree with the Examiner that a "single family," given a broad but reasonable interpretation, includes "any group of related things," such as all devices networked within the boundaries of a campus. *See* Ans. 18.

Appellant argues that "[t]he term 'domain' already connotes a group of related things. Interpreting 'a single family' to mean nothing more than

‘any group of related things’ renders the ‘single family’ limitation redundant, and thus meaningless.” Reply Br. 4. However, Appellant does not provide sufficient persuasive evidence that a domain is limited to a group of related things, nor does the Specification provide a special definition for “domain.” Thus, we find that a domain, given a broad but reasonable interpretation encompasses any composition or aggregation of things, related or unrelated. Here, the Examiner’s interpretation of “a single family” as a group of related things provides additional meaning by limiting the claimed domain to a composition or aggregation of related network devices, such as those networked within the boundaries of a campus. Therefore, we agree with the Examiner that Roesse, which defines restrictions such as a “room,” “building,” or “campus,” discloses “wherein said domain comprises networked devices associated with a single family,” as recited in claim 4. *See* Ans. 5 (citing Roesse ¶ [0115]).

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 4, and dependent claims 7 – 10 and 30, with respect to this issue. Appellant makes similar arguments with respect to claims 9, 13, and 16. *See* App. Br. 15, 16, and 18. For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claims 9, 13, and 16, with respect to this issue.

ISSUE 4

With respect to claim 7, Appellant argues that the relied-upon disclosures in Roesse “concern restricting network log-ins based on a user’s GPS- or other location-authenticated information. They do not concern re-

distribution of entertainment content from an intended destination address to a second address.” App. Br. 13; *see also* Reply Br. 5.

Issue

Did the Examiner err in finding that Roesse discloses “the additional data includes a field signaling that copying of data in said packet to said second destination address should be: (a) permitted if the second physical location is physically proximate to the first physical location; and (b) prohibited if the second physical location is physically remote from the first physical location,” as recited in claim 7?

Analysis

The Examiner finds that Roesse, by describing a location limitation in terms of physical location, discloses the claimed field signaling whether a copying of data is permitted or prohibited based on whether a second physical location is physically proximate to or remote from a first physical location. *See* Ans. 5 (citing Roesse ¶¶ [0100] – [0103]). The Examiner acknowledges that “a small portion of the cited paragraphs of Roesse does explain that logins are an expanded feature of the authentication/location server’s location database.” Ans. 18. However, the Examiner identifies additional disclosures as providing more detailed explanations showing that Roesse discloses the claimed field. *See id.* (citing Roesse ¶¶ [0096] – [0099]).

Appellant argues that the additional disclosures cited “do not teach that copying of data in a packet should be permitted only if the destination physical location is physically proximate to the first physical location.” Reply Br. 5. However, Roesse discloses that “[i]f an attempt is made to access [sensitive] information from what is otherwise an authenticated

device, that information or file may nevertheless be destroyed *if the authenticated device is not at a specified location or region.*” Roese ¶ [0096]. Roese further discloses that “system 100 may be programmed to deny access . . . upon request from a network entry device, or coming through an intermediate device that is located outside of a specified region.” *Id.* That is, Roese discloses restricting the copying of data (prohibiting access) if a second physical location (the location of an intermediate device) is physically remote from the first physical location (the location of the network entry device). Therefore, we agree with the Examiner that Roese discloses “the additional data includes a field signaling that copying of data in said packet to said second destination address should be: (a) permitted if the second physical location is physically proximate to the first physical location; and (b) prohibited if the second physical location is physically remote from the first physical location,” as recited in claim 7.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 7, and dependent claims 8 and 9, with respect to this issue. Appellant makes similar arguments with respect to claim 14. *See* App. Br. 16 – 17. For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 14, and dependent claims 16 and 17, with respect to this issue.

ISSUE 5

With respect to claim 8, Appellant argues that “Roese’s Figs. 1 and 8 have no teachings about a common domain.” App. Br. 14.

Issue

Did the Examiner err in finding that Roesse discloses “wherein the first and second destination addresses are within a common domain,” as recited in claim 8?

Analysis

The Examiner finds that in the campus boundary example of Roesse, “the first and second devices that are ‘verified and authenticated’ are in a common ‘domain’, or within a group of networked computers.” Ans. 19 (citing Roesse fig. 8).

Appellant argues that the Examiner erroneously “conflates network address domains and physical locations.” Reply Br. 6. In particular, Appellant argues that “[t]he claimed ‘common domain’ refers to a network address-sense of the term,” Reply Br. 5—that a physical location, such as a campus boundary does not anticipate a network address domain, Reply Br. 6. However, we agree with the Examiner that the Specification “supplies no definition for ‘common domain.’” Ans. 19. Furthermore, Appellant does not provide sufficient persuasive evidence that the claimed domain is limited to a network address domain. Thus, we agree with the Examiner that a broad but reasonable interpretation of addresses within a “common domain” includes the addresses of devices within a defined boundary.

Roesse discloses a network that is location-aware. *See* Roesse ¶ [0129] and fig. 8. The connection points of devices are used to determine the locations of devices in the system. *See* Roesse ¶ [0134]. Thus, Roesse discloses devices (first and second addresses) in a common domain (within a defined boundary of a location-aware network). Therefore, we agree with

the Examiner that Roesse discloses “wherein the first and second destination addresses are within a common domain,” as recited in claim 8.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 8, with respect to this issue. Appellant makes similar arguments with respect to claim 15. *See* App. Br. 17. For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 15, with respect to this issue.

ISSUE 6

With respect to claim 17, Appellant argues that “Roesse’s firewall is a way to enforce location-based restrictions determined by the ‘location aware’ features of his system.” App. Br. 18. Appellant argues that “Roesse does not – in whole or in part – use a firewall to *define* a geographical boundary, across which certain content should not pass.” Reply Br. 8.

Issue

Did the Examiner err in finding that Roesse discloses “determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address,” as recited in claim 17?

Analysis

The Examiner correctly finds that Roesse “describes combining the use of a firewall with the physical locations of the devices, where it states a firewall makes determination of packets into and out of a network.” Ans. 7 (citing Roesse ¶ [0098]). In particular, Roesse discloses that “[f]irewalls (e.g.,

140 (FIG. 8)) also provide a technique for network usage regulation. Firewalls are primarily computer programs designed to analyze packets and, from that analysis, make a determination as to *whether packet transmission into or out of the network is permitted.*” Roese ¶ [0098] (emphasis added). Contrary to Appellant’s arguments, Roese’s firewalls, by establishing which packet transmissions cross into or out of a location-aware network, define the location-aware network’s boundary. *Id.* Therefore, we agree with the Examiner that Roese discloses “determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common firewall with the first destination address,” as recited in claim 17.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 17, with respect to this issue. Appellant makes similar arguments with respect to claim 1. *See App. Br. 19.* For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 1, with respect to this issue.

ISSUE 7

With respect to claim 1, Appellant argues that the cited portions of Roese lack “any teaching of single-bit flags.” App. Br. 20. Appellant further argues “that the construction being implicitly argued by the Office (e.g., that all data representations are a series of single bit flags) renders the ‘single-bit flags’ limitation meaningless.” Reply Br. 8.

Issue

Did the Examiner err in finding that Roese teaches or suggests “determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more single-bit flags included in the header data of said packet,” as recited in claim 1?

Analysis

As discussed above, the Examiner correctly finds that Roese describes the use of tags that establish boundary restrictions. *See also* Ans. 9 (citing Roese ¶ [0115] – [0118] and fig. 6). The Examiner further finds that the representation of restriction information using one or more bits teaches or suggests the claimed “one or more single-bit flags,” as broadly recited. *See* Ans. 23. Appellant does not persuasively distinguish between bits representing boundary restriction tags and one or more single-bit flags.

Furthermore, the location restrictions represented by a tag provide additional restriction details that teach or suggest one or more single-bit flags. For example, Roese teaches that “[t]he tag may be configured either to deny opening (step 620a) of the transmitted data at an unauthorized location, or to destroy (step 620b) the data when it is determined that the data is in an unauthorized location.” Roese ¶ [0116]. In other words, Roese distinguishes between data that may cross a boundary, but must not be accessible outside that boundary, and data that may not cross a boundary, and must be destroyed if it were to cross that boundary. The distinction between denying-access-to versus destroying data teaches or suggests one or more single-bit flags. Therefore, we agree with the Examiner that Roese teaches or suggests “determining whether an IP packet should be regarded as conveying content

that should not cross said boundary, by reference to one or more single-bit flags included in the header data of said packet,” as recited in claim 1.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 1, with respect to this issue.

ISSUE 8

With respect to claim 1, Appellant argues that the Examiner erred in relying on the combined teachings and suggestions of Roese and Levy ’899 because the Examiner’s “rationale for the combination *presumes* that the content is *already* watermarked,” but Roese does not teach a watermark. *See* App. Br. 21; *see also* Reply Br. 9 – 10.

Issue

Did the Examiner err in finding that the combination of Roese and Levy ’899 teaches or suggests “wherein said one or more flag bits are related to the payload of a watermark in the content data,” as recited in claim 1?

Analysis

The Examiner acknowledges that “Roese does not explicitly state placing the additional data as a packet header containing flag bits being ‘related to the payload of a watermark in the content.’” Ans. 9. Instead, the Examiner relies on Levy ’899 to teach or suggest header information pertaining to a watermark payload. *See id.* We agree with the Examiner that Appellant cannot show error in the Examiner’s rejection by attacking Roese alone, since the rejection relies on the combined teaching and suggestions of Roese and Levy ’899. *See* Ans. 23.

Furthermore, Levy ’899 teaches that a “watermark signal may be decoded and re-encoded in the individual packets, or re-encoded after the

signal is re-combined. The re-encoding is effected by transferring *a watermarking command in the header of the packets specifying the watermark payload* and watermark embedding protocol to be used in the re-combined signal.” Levy ’899 ¶ [0035]. That is, Levy ’899 teaches or suggests packet header data related to the payload of a watermark in the content data. *See also* Levy ’899 ¶ [0016] (“Transmarking may include converting an out of band identifier like a tag in a header/footer to a watermark or vice versa”). Thus, the Examiner properly relies on Levy ’899 to show that it would have been obvious to an artisan of ordinary skill in the art to use the payload of a watermark in content data as the source for packet header data. The modification of Roesse’s location-based access control using tags with transmission restrictions to use watermark payloads as sources for those transmission restrictions merely represents the combination of familiar elements to yield predictable results. *See KSR Int’l, Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007). Therefore, we agree with the Examiner that the combination of Roesse and Levy ’899 teaches or suggests “wherein said one or more flag bits are related to the payload of a watermark in the content data,” as recited in claim 1

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 1, with respect to this issue. Appellant makes similar arguments with respect to claims 10, 18, and 25. *See* App. Br. 23 – 25. For the reasons discussed above, we also do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 10, 18, and 25, and dependent claims 26 – 28, with respect to this issue.

ISSUE 9

With respect to claim 25, Appellant argues that “Roese does not teach a home networking device that refuses to transmit packets ‘to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer’s home network.’” App. Br. 24. In particular, Appellant argues that “[t]he only reference to a ‘home’ in Roese is as a recipient of content – not as a redistributor.” Reply Br. 10.

Issue

Did the Examiner err in finding that Roese teaches or suggests “refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer’s home network,” as recited in claim 25?

Analysis

The Examiner correctly finds that Roese teaches a firewall that refuses to redistribute content from a domain. *See* Ans. 25 (citing Roese fig. 8). In particular, Roese teaches the use of a firewall to determine “whether packet transmission into or out of the network is permitted.” Roese ¶ [0098]. The Examiner also correctly finds that domains taught or suggested by Roese include, for example, “a room, building (or house), or campus.” Ans. 25; *see also* Roese ¶ [0115]. We agree with the Examiner that Roese’s teaching of a building as a domain teaches or suggests a home (a type of building) as a domain. Therefore, we agree with the Examiner that Roese teaches or suggests “refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment

should not be redistributed from the consumer's home network," as recited in claim 25.

Accordingly, we do not find Appellant's arguments persuasive of error in the Examiner's rejection of claim 25, and of dependent claims 26 – 28, with respect to this issue.

ISSUE 10

With respect to claim 26, Appellant argues that Levy '899 fails to teach or suggest the parent claim 25 requirement that extracting restriction information from packet header data precede including data related to the restriction in header portions of each of the claimed IP packets. *See* App. Br. 25; *see also* Reply Br. 12.

Issue

Did the Examiner err in finding that the combination of Roese and Levy '899 teaches or suggests "wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment," as recited in claim 26?

Analysis

The Examiner finds that "Roese does not explicitly state 'extracting restriction information from header data conveyed with the video entertainment . . . and 'including data indicating said ascertained restriction information in header portions of each said IP packets.'" Ans. 11. Instead the Examiner relies on Levy '899 to teach or suggest such extraction. *See id.* (citing, e.g., Levy '899 ¶¶ [0015] and [0023]). We agree with the Examiner that Levy '899 teaches or suggests extracting restriction information from header data. In particular, Levy '899 teaches that "[t]ransmarking may

include converting an out of band identifier like a tag in a header/footer to a watermark or vice versa.” Levy ’899 ¶ [0016]. That is, header content can contain extractable and transmittable restriction information. Therefore, we agree with the Examiner that the combination of Roesse and Levy ’899 teaches or suggests “wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment,” as recited in claim 26.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 26, with respect to this issue.

ISSUE 11

With respect to claim 28, Appellant argues that Levy ’899 fails to teach or suggest the parent claim 25 requirement that discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment precede including data related to the restriction in header portions of each of the claimed IP packets. *See App. Br. 26; see also Reply Br. 13.*

Issue

Did the Examiner err in finding that the combination of Roesse and Levy ’899 teaches or suggests “wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment,” as recited in claim 28?

Analysis

The Examiner’s findings with respect to claim 28 are similar to the Examiner’s findings with respect to claim 26, discussed above. *See Ans. 11.*

In addition, the Examiner finds that “Roese does not explicitly state . . . ‘discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.’” *Id.* Instead the Examiner relies on Levy ’899 to teach or suggest such discerning. *See id.* (citing, e.g., Levy ’899 ¶¶ [0022] – [0023]). We agree with the Examiner that Levy ’899 teaches or suggests discerning restriction information from digital watermark information. As discussed above, Levy ’899 teaches that “[t]ransmarking may include converting an out of band identifier like a tag in a header/footer to a watermark or vice versa.” Levy ’899 ¶ [0016]. That is, watermark content can contain discernable restriction information. Levy also explicitly teaches detecting and decoding a watermark in a watermarked signal. *See* Levy ’899 ¶¶ [0022] – [0023] and fig. 1. Therefore, we agree with the Examiner that the combination of Roese and Levy ’899 teaches or suggests “wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment,” as recited in claim 28.

Accordingly, we do not find Appellant’s arguments persuasive of error in the Examiner’s rejection of claim 28, with respect to this issue.

ISSUE 12

With respect to claim 27, Appellant argues “the claim requires that the restriction information is included in header portions of the IP packets. As such, it is not hidden. Since it is not hidden, the Final Rejection provides no indication why an artisan would have turned to Levy ’899 for watermark teachings.” App. Br. 27. Appellant further argues that “the rationale for

combining Levy '844 with Roese and Levy '899 in the claimed manner is impermissibly based on hindsight, rather than the required 'articulated reasoning with some rational underpinning.'" Reply Br. 13.

Issue

Did the Examiner err in concluding that it would have been obvious to an artisan of ordinary skill to combine the teachings and suggestions of Roese, Levy '899, and Levy '844 to teach or suggest the recitations of claim 27?

Analysis

Appellant's argument that "the claim requires that the restriction information is included in header portions of the IP packets," App. Br. 27, is not commensurate with the recitations of claim 27, which are directed to limiting the ascertaining to include "wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment." Furthermore, the Examiner makes specific findings showing that it would have been obvious to combine the teachings and suggestions of Roese, Levy '899, and Levy '844 to teach or suggest the recitations of claim 27. *See, e.g.*, Ans. 12 – 13. Appellant does not provide sufficient persuasive arguments or evidence to rebut these findings or to support the conclusory statement that the Examiner erroneously relies on impermissible hindsight reasoning. Therefore, we find the Examiner did not err in concluding that it would have been obvious to an artisan of ordinary skill to combine the teachings and suggestions of Roese, Levy '899, and Levy '844 to teach or suggest the recitations of claim 27.

Appeal 2010-007767
Application 10/797,920

Accordingly, we do not find Appellant's arguments persuasive of error in the Examiner's rejection of claim 27, with respect to this issue.

DECISION

We affirm the Examiner's decision to reject claims 1, 4, 7 – 11, 13 – 18, and 25 – 31.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

tj