



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.
13/734,175	01/04/2013	Craig S. ETCHEGOYEN	UN-NP-SC-083	1018
96051	7590	11/25/2016	EXAMINER	
Uniloc USA Inc. Legacy Town Center 7160 Dallas Parkway Suite 380 Plano, TX 75024			LAGOR, ALEXANDER	
			ART UNIT	PAPER NUMBER
			2491	
			NOTIFICATION DATE	DELIVERY MODE
			11/25/2016	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sean.burdick@unilocusa.com
tkiatkulpiboone@unilocusa.com
kris.pangan@unilocusa.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CRAIG S. ETCHEGOYEN,
DONO HARJANTO, and SEAN D. BURDICK

Appeal 2015-007726
Application 13/734,175¹
Technology Center 2400

Before HUNG H. BUI, DANIEL J. GALLIGAN, and
MICHAEL J. ENGLE, *Administrative Patent Judges*.

GALLIGAN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner’s final rejection of claims 1–5. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.²

¹ The Appeal Brief identifies Uniloc Luxembourg S.A. as the real party in interest. App. Br. 3.

² Our Decision refers to Appellants’ Appeal Brief, filed March 9, 2015 (“App. Br.”); Appellants’ Reply Brief, filed August 21, 2015 (“Reply Br.”); Examiner’s Answer, mailed June 29, 2015 (“Ans.”); Final Office Action, mailed September 8, 2014 (“Final Act.”); and Appellants’ Specification, filed January 4, 2013 (“Spec.”).

STATEMENT OF THE CASE

Appellants' invention relates to "a method and system for implementing zone-restricted behavior of a computing device." Spec. ¶ 2.

Claims 1 and 3 are independent claims. Claim 1 is reproduced below:

1. A method for implementing zone-restricted behavior of a computing device, the method comprising:

identifying wireless access points using the computing device;

determining, by the computing device, a number of authorized wireless access points from the identified wireless access points by receiving digital fingerprints of the identified wireless access points and comparing each of the received digital fingerprints to digital fingerprints of authorized wireless access points;

determining that the computing device is located within a restricted access zone when the number of authorized wireless access points accessible by the computing device from a fixed location exceeds a predetermined threshold of authorized wireless access points; and

enabling a zone mode of the computing device when the computing device is determined to be located within the restricted access zone.

References

Nguyen et al.	US 2008/0076572 A1	Mar. 27, 2008
Bradley	US 2011/0090896 A1	Apr. 21, 2011

Examiner's Rejection

Claims 1–5 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nguyen and Bradley. Final Act. 14–21.

ANALYSIS

Claims 1 and 5

Appellants contend Nguyen does not teach “identifying wireless access points using the computing device,” as recited in claim 1. App. Br. 6–7; Reply Br. 2–4. According to Appellants, “*Nguyen’s* methods operate based upon mobile device detection of wireless access points by mobile gaming devices, but not by identifying the wireless access points.” App. Br. 7. Appellants cite dictionary definitions of “identify” and “identity” and argue that the identifying step requires the computing device to uniquely identify wireless access points and differentiate among individual wireless access points. App. Br. 7.

In response, the Examiner finds Nguyen’s disclosure of distinguishing wireless access points that are associated with a first zone versus a second zone based on different types of heartbeats emitted by the access points teaches “identifying” within the meaning of claim 1. Ans. 10–11 (citing Nguyen ¶ 12). Nguyen discloses:

At a basic level, areas where mobile wager gaming is allowed, for example casino floors, nightclubs, and bars, have an underlying zone which has transmitters or antennas that transmit a security signal to the gaming device which allows the device to execute game play. As long as the device is in that zone it will hear the beacon or heartbeat from the transmitter and allow game play. If the device is taken to an area where wagering games are not allowed, for example, a video arcade, a hotel room, a family-style restaurant, the underlying zone may have *transmitters that send a different type of heartbeat* that tells the device that wagering game play is not allowed while other services are allowed, such as non-wager game play, concierge services, viewing restaurant menus and video entertainment, and the like.

Nguyen ¶ 12 (emphasis added).

We agree with the Examiner that the broadest reasonable interpretation of the term “identifying wireless access points” recited in Appellants’ claim 1 encompasses distinguishing access points based on types of signals as disclosed by Nguyen. Appellants cite various passages of the specification in an attempt to support their interpretation of “identifying.” Reply Br. 2–3. For example, Appellants argue: “To determine location, the disclosure states that the ‘computing device utilizes the wireless access point identifiers to *identify* the authorized wireless access points.[’] (Emphasis added.) See ¶ 11.” Reply Br. 2. However, Appellants omit the preceding sentence, which provides context for the cited disclosure:

It is particularly challenging to distinguish between a computing device just inside a restricted access zone and one just outside the restricted access zone, both of which are connected to a local area network wirelessly. To make this distinction, each of one or more authorized wireless access points within the restricted access zone transmits wireless access point identifiers. The computing device utilizes the wireless access point identifiers to identify the authorized wireless access points.

Spec. ¶ 9.³ Thus, this instance of identifying is concerned with distinguishing access points associated with different zones, which is what the Examiner finds Nguyen teaches. Therefore, this instance of “identifying” in Appellants’ Specification does not distinguish the claimed “identifying” step from the disclosure of Nguyen.

Appellants also point to their Specification’s disclosure regarding a “digital fingerprint” as a unique identifier of a wireless access point. Reply Br. 3 (citing Spec. ¶ 40). However, “digital fingerprints” are explicitly

³ It appears Appellants use paragraph numbers from the published application. Our Decision refers to the paragraph numbers in the application as filed.

recited only in the second step of claim 1, which is directed to “determining . . . a number of authorized wireless access points.” Claim 1 does not recite that the “identifying” step must use “digital fingerprints.” Moreover, as we discuss below, the Examiner relies on Bradley to teach “digital fingerprints,” and, therefore, Appellants’ arguments that Nguyen does not teach such identifiers are not responsive to the Examiner’s findings. *See* Final Act. 15–16.

Appellants further contend Nguyen does not teach “determining . . . a number of authorized wireless access points from the identified wireless access points,” as recited in claim 1. App. Br. 8–9; Reply Br. 4–5. According to Appellants, “*Nguyen* provides no teaching or suggestion that the mobile device should distinguish authorized transmitters from unauthorized transmitters.” App. Br. 8, 9.

We disagree. As the Examiner explains, Nguyen discloses transmitters that emit different types of heartbeats that enable the device to unlock certain functionality depending on the heartbeat received. Ans. 11–12 (citing Nguyen ¶ 12). The Examiner further explains that “if a guest takes the wagering device to an area with ‘*transmitters that send a different type of heartbeat*’ (i.e. unauthorized transmitters for the purposes of permitting wagering game play), the device restricts game play.” Ans. 11 (citing Nguyen ¶ 12). Nguyen discloses: “If the device is taken to an area where wagering games are not allowed . . . the underlying zone may have transmitters that send a different type of heartbeat that tells the device that wagering game play is not allowed while other services are allowed” Nguyen ¶ 12. We agree with the Examiner that this disclosure of Nguyen

teaches distinguishing authorized transmitters from unauthorized transmitters.

Appellants also contend Nguyen does not teach or suggest “determining that the computing device is located within a restricted access zone when the number of authorized wireless access points accessible by the computing device from a fixed location exceeds a predetermined threshold of authorized wireless access points.” App. Br. 10–11. We are not persuaded. Claim 1 does not recite what the threshold number is that must be met in order to determine that the device is in a restricted access zone. Therefore, determining that the device is in a restricted access zone when only one authorized wireless access device is accessible from a fixed location is within the scope of this “determining” step. *See* Final Act. 7 (“Since it merely is a number, the number by itself could be a single device.”). Nguyen discloses determining that the mobile gaming device is in a restricted access zone if only one authorized transmitter is accessible to it. *See* Nguyen ¶ 12 (“As long as the device is in that zone it will hear the beacon or heartbeat from the transmitter and allow game play.”). Thus, we disagree with Appellants’ contention.

Appellants still further contend Bradley does not teach or suggest a computing device “receiving digital fingerprints of the identified wireless access points and comparing each of the received digital fingerprints to digital fingerprints of authorized wireless access points.” App. Br. 11–12. Appellants argue “the UUIDs [universally unique identifiers] that are broadcast by *Bradley’s* participant access points are received only by the other participant access points, and not by any computing devices,” and, therefore, “there is no teaching or suggestion in *Bradley* that a computing

device (or an access point) receive UUIDs and compare them to authorized UUIDs.” App. Br. 12.

We are not persuaded by these arguments because the Examiner relies on Bradley’s disclosure of unique identifiers for access points *in combination with* Nguyen’s disclosure of the mobile gaming device’s detecting and identifying wireless access points based on different signals received, as discussed above. The Examiner finds that “Nguyen already discloses the use of ‘heart beats’ to differentiate between different zones” and explains that “it would be even more efficient to use fingerprints of [Bradley] that identif[y] the wireless access points to permit a more fine grained access control of the devices.” Ans. 15. We find this to be articulated reasoning with rational underpinning underlying the conclusion of obviousness, and we find this reasoning to be supported by the evidence of record. For example, Nguyen identifies the need for zone differentiation (¶ 72) and describes that areas of a casino may be changed even temporarily to restrict or allow certain mobile device activity (¶ 49). Nguyen describes that further granularity may be beneficial to allow different classes of wagering games. *See* Nguyen ¶ 53 (“In some implementations, the type of wagering game play allowed (e.g., Class II or Class III) is based on the zone in which the mobile device is located.”). Nguyen still further describes:

[A] “customized” functionality level can be created for a weekend poker event where participants can only play a new variation of poker and can only order certain food and drinks from a vendor sponsoring the event. As can be seen, there can be dozens of pre-defined and ad hoc levels of functionality defined in the mobile gaming network of the present invention.

Nguyen ¶ 53. Thus, Nguyen’s disclosure of the benefits of various levels of zone differentiation supports the Examiner’s determination that a person of

ordinary skill in the art would have had reason to incorporate digital fingerprints, such as the unique identifiers in Bradley, into the system of Nguyen to facilitate more granular access control and greater zone differentiation.

Based on the foregoing, Appellants' arguments that there would have been no reason to combine the teachings of Nguyen and Bradley are not persuasive. *See* App. Br. 13–14; Reply Br. 6. Appellants argue that Bradley “is directed to synchronizing data in a network” and “the Examiner has not explained how or why a skilled artisan would modify *Nguyen's* system of beacon signals to synchronize wireless access control settings, much less how such modification would require an exchange of UUID amongst the various access points.” Reply Br. 6. However, as discussed above, the Examiner's rejection is based on Bradley's disclosure of unique identifiers (digital fingerprints), not on Bradley's disclosure of data synchronization.

We further disagree with Appellants' contention that the UUID in Bradley is not sufficiently unique to be a digital fingerprint. Reply Br. 5. Bradley discloses:

The use of UUIDs may enable a network such as network 11 to uniquely identify multiple access points without central coordination and without needing to resolve name conflicts. For example, the participant ID may be converted to a participant UUID using a name-based hash function. The hash function may be a function of an access point's media access control (MAC) address, serial number, and any other data that uniquely identifies the access point.

Bradley ¶ 45 (cited at Final Act. 16). This description is consistent with Appellants' Specification, which states that “a digital fingerprint is a unique identifiers [sic] of an individual computing device that is derived from data stored on the device that identifies individual components of hardware or

software or the system configuration of the device.” Spec. ¶ 41. The Specification further states that the device fingerprint can be generated by “hashing” device-specific data, such as “serial numbers.” *See id.* ¶¶ 42–43.

We find the Examiner’s conclusion of obviousness to be consistent with the Supreme Court’s guidance that “if 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.” *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 417 (2007); *see also id.* at 416 (“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.”). Appellants have not presented evidence sufficient to show that combining the prior art was “uniquely challenging or difficult for one of ordinary skill in the art” or “represented an unobvious step over the prior art.” *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418–19). Nor have Appellants presented evidence that any of their incorporations of known limitations yielded more than expected results.

We are not persuaded the Examiner erred in concluding the subject matter of claim 1 would have been obvious over the combination of Nguyen and Bradley. Therefore, we sustain the rejection of claim 1 under 35 U.S.C. § 103(a), as well as the rejection of claim 5, for which Appellants present no additional argument. *See App. Br.* 19.

Claim 2

Appellants’ contentions with respect to claim 2 also do not persuade us the Examiner erred in concluding the subject matter would have been obvious. *See App. Br.* 14–16. Referring to paragraph 18 of Nguyen,

Appellants acknowledge “*Nguyen* discloses a security signal emanating from a gaming server which signal contains information in the form of an ID of the mobile device,” but they argue “the security signal does not emanate from an access point, contains no information about an access point, and does not result in (nor in any way facilitate) identification and authorization of an access point to a gaming device.” App. Br. 15. This argument, however, does not address the disclosure of paragraph 60 of *Nguyen*, which the Examiner also relied upon to reject claim 2. *See* Final Act. 17–18 (citing *Nguyen* ¶¶ 12, 15, 18, 60).

Nguyen discloses:

In a preferred embodiment, *NFM communication is used to transmit a security signal originating from a network component, such as a mobile gaming server, to a mobile gaming device. As described in greater detail below, NFM signals emanate from antennas in a zone and are received by a mobile gaming device that is within two meters of the antenna.*

Nguyen ¶ 60 (emphasis added). In the Answer, the Examiner explains, and we agree, that based on this disclosure, “*Nguyen* teaches how a security signal that originates from a mobile gaming server is received by a mobile gaming device from antennas (as depicted in Fig. 3).” Ans. 16. Because *Nguyen* teaches a signal being relayed through an antenna (“access point”), Appellants’ contention that “the security signal does not emanate from an access point” is incorrect. *See* App. Br. 15.

Furthermore, as discussed above with respect to claim 1, *Nguyen* teaches identifying authorized access points based on signals (“heartbeats”) received from transmitters. *See, e.g.*, *Nguyen* ¶ 12. Therefore, we disagree with Appellants’ contention that “the security signal . . . contains no information about an access point, and does not result in (nor in any way

facilitate) identification and authorization of an access point to a gaming device.” *See* App. Br. 15.

We are also unpersuaded by Appellants’ contention that “neither *Nguyen* alone nor *Nguyen* in combination with *Bradley* teaches the latter part of this claim 2 element, that of ‘receiving verification from the restricted access server.” App. Br. 16. The Examiner has shown that *Nguyen* teaches signals originating from a gaming server going through antennas or transmitters to a gaming device, resulting in the gaming device’s determination that gaming is or is not allowed in a particular zone. *See* Final Act. 17–18 (citing *Nguyen* ¶¶ 12, 15, 18, 60); Ans. 15–16; *see also* discussion of claim 1 above.

We are not persuaded the Examiner erred in concluding the subject matter of claim 2 would have been obvious over the combination of *Nguyen* and *Bradley*. Therefore, we sustain the rejection of claim 2 under 35 U.S.C. § 103(a).

Claim 3

With respect to independent claim 3, Appellants argue “[n]either *Nguyen* alone nor *Nguyen* in combination with *Bradley* teaches the use of signal strength received from identified and authorized wireless access points.” App. Br. 17. Claim 3, however, recites no such limitation. Rather, claim 3 requires “detecting signal strength of each of a number of wireless access points.” We agree with the Examiner that *Nguyen* teaches this limitation. *See* Final Act. 18 (citing ¶ 61 (“The signal strength attenuates or falls off at a ratio of $1/r(6)$ as the distance from an antenna increases”).

Appellants also advance arguments similar to those for claim 1 that there would have been no reason to combine the teachings of *Nguyen* and

Bradley because Bradley teaches identifying access points to one another, not to a computing device. *See* App. Br. 17–18. As we explain above with respect to claim 1, the Examiner relies on Bradley’s disclosure of unique identifiers for access points *in combination with* Nguyen’s disclosure of the mobile gaming device’s detecting wireless access points. *See* Final Act. 18–20. For the reasons explained with respect to claim 1, we are not persuaded the Examiner erred in combining the teachings of Nguyen and Bradley.

We are not persuaded the Examiner erred in concluding the subject matter of independent claim 3 would have been obvious over the combination of Nguyen and Bradley. Therefore, we sustain the rejection of claim 3 under 35 U.S.C. § 103(a).

Claim 4

Claim 4 depends from claim 1 and recites “identifying only wireless access points which have a signal strength greater than a predetermined signal strength threshold.” Appellants argue “[t]here is no teaching or suggestion in *Nguyen* that the identification of wireless access points by the computing device be restricted based on signal strength.” App. Br. 19. We disagree. Nguyen describes that signals from access points become attenuated as distance from the access point increases such that, at certain distances, the signal strength is such that the access point cannot be identified. Nguyen discloses:

The signal strength attenuates or falls off at a ratio of $1/r(6)$ as the distance from an antenna increases, as represented by the circular lines emanating from the end of the antennas shown in FIG. 3. An outer line 320 shows where the signal becomes too weak to be detectable for most practical applications. For example, at three meters, the strength of a NFM signal is 0.14% of the original signal strength.

Appeal 2015-007726
Application 13/734,175

Nguyen ¶ 61; Ans. 13 (quoting Nguyen ¶ 61 but mislabeling it as ¶ 60). Thus, we agree with the Examiner that Nguyen teaches or suggests a predetermined signal strength threshold beyond which wireless access points will not be identified (e.g., the signal strength at outer line 320).

We are not persuaded the Examiner erred in concluding the subject matter of dependent claim 4 would have been obvious over the combination of Nguyen and Bradley. Therefore, we sustain the rejection of claim 4 under 35 U.S.C. § 103(a).

DECISION

We affirm the Examiner's decision to reject claims 1–5.

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