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.
14/615,129	02/05/2015	Mitri ABOU-RIZK	VERV-003/01US 305990-2014	1030

58249 7590 01/24/2019

COOLEY LLP
ATTN: IP Docketing Department
1299 Pennsylvania Avenue, NW
Suite 700
Washington, DC 20004

EXAMINER	
PAN, PEILIANG	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
01/24/2019	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):

zIPPatentDocketingMailboxUS@cooley.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MITRI ABOU-RIZK, BRIAN CROOK,
ERIC M. JOHNSTON, GARY NG, and CHRIS NICOTRA

Appeal 2017-003849
Application 14/615,129[1]
Technology Center 2400

Before KALYAN K. DESHPANDE, JASON V. MORGAN, and HUNG H. BUI, *Administrative Patent Judges*.

BUI, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–24, which are all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.[2]

---

[1] According to Appellants, the real party in interest is Verve Wireless, Inc. App. Br. 3.

[2] Our Decision refers to Appellants' Appeal Brief ("App. Br.") filed July 12, 2016; Reply Brief ("Reply Br.") filed January 3, 2017; Examiner's Answer ("Ans.") mailed November 3, 2016; Final Office Action ("Final Act.") mailed October 28, 2015; and original Specification ("Spec.") filed February 5, 2015.

STATEMENT OF THE CASE

Appellants' invention relates to "methods and apparatus for evaluating location data, detecting spoofed location data, and/or assigning accuracy scores to location data." Spec. ¶ 105. Claims 1–24 are pending on appeal. Claims 1 and 16 are independent. Claim 1 illustrates the claimed subject matter, as reproduced below, with disputed limitations in *italics* and bracketing added:

> 1. An apparatus, comprising:
>
> a network module configured to [1] *receive a signal identifying an untrusted location, the untrusted location associated with a mobile communication device*, the untrusted location having an unknown accuracy;
>
> a first data source comparator module implemented in at least one of a processor or a memory, the first data source comparator module configured to compare the untrusted location to a database of known spoofed locations to define a first match when the untrusted location matches a known spoofed location from the database;
>
> [2] *a second data source comparator module* implemented in at least one of a processor or memory, the second data source comparator module configured to *compare the untrusted location to a plurality of locations previously received by the network module to define a second match when the untrusted location is statistically overrepresented in the plurality of locations*; and
>
> [3] *a spoofed location detection module* operably coupled to the first data source comparator module, the second data source comparator module, and the network module, the spoofed location detection module configured to
>
> [3a] *determine if the untrusted location was determined by the mobile communication device*, the spoofed location detection module configured to
>
> [3b] *determine based, at least in part, on at least one of (1) the first match, or (2) the second match.*

App. Br. 18 (Claims App.).

EXAMINER'S REJECTIONS and REFERENCES

(1) Claims 1–7 and 9–20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thomson et al. (US 2010/0134352 A1; published June 3, 2010; "Thomson"), Liu et al. (US 2012/0304292 A1; published Nov. 29, 2012; "Liu"), and Varoglu (US 2014/0232593 A1; published Aug. 21, 2014). Final Act. 3–11.

(2) Claims 8 and 21–24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thomson, Liu, Varoglu, and Martin et al. (US 2012/0309408 A1; published Dec. 6, 2012; "Martin"). Final Act. 12–16.

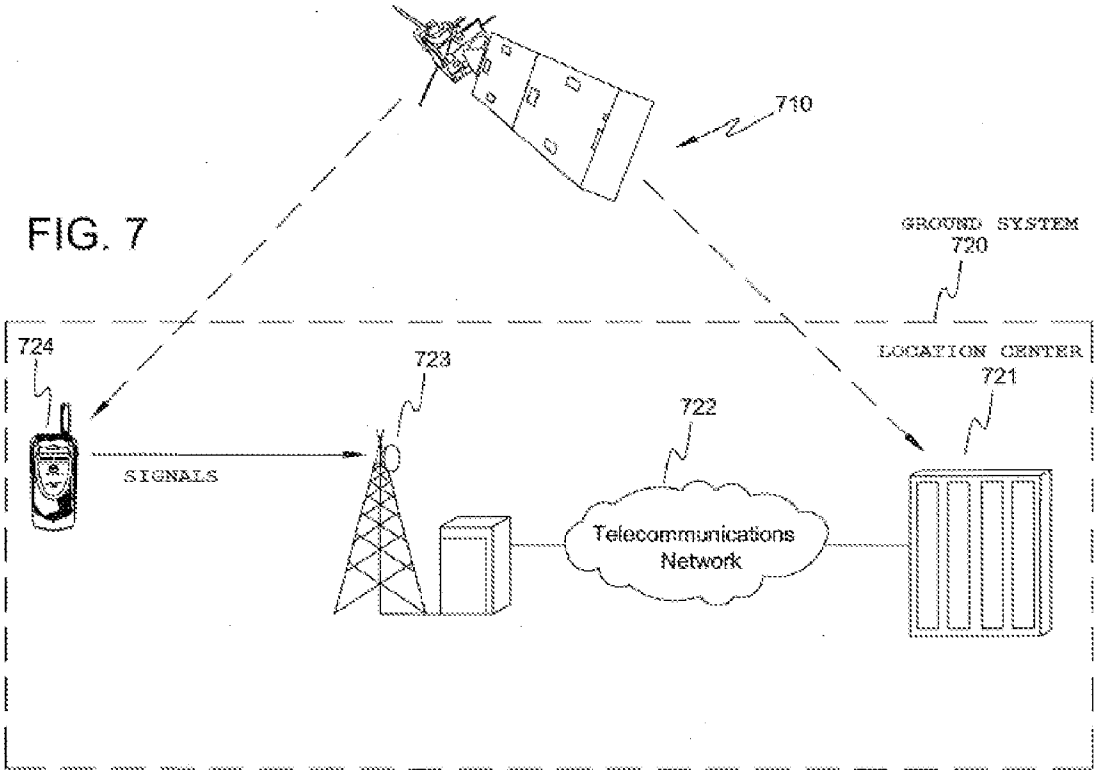
ANALYSIS

In support of the obviousness rejection of claim 1 and, similarly, claim 16, the Examiner finds the combination of Thomson, Liu, and Varoglu teaches all the claim limitations. Final Act. 3–7. In particular, the Examiner finds Thomson teaches most aspects of Appellants' claimed apparatus (shown in Figure 7) to determine whether satellite measurements transmitted from a mobile device have been forged, including:

> (1) "a network module . . . to receive a signal identifying an untrusted location . . . associated with a mobile . . . device";
>
> (2) "a data source comparator module . . . to compare the untrusted location to [a location defined by the network module] to define a match . . ."; and
>
> (3) "a spoofed location detection module . . . to determine if the untrusted location was determined by the mobile . . . device . . . based, at least in part on at least the first match."

Final Act. 3–4 (citing Thomson ¶ 41).

Thomson's Figure 7 is reproduced below with additional markings for illustration:



Thomson's Figure 7 shows an apparatus for determining whether mobile device 724 transmitted a forged satellite measurement.

As shown in Figure 7, location center 721 includes a GPS receiver (not shown) to receive signals (including one or more satellite measurements and GPS navigation data message) transmitted from mobile device 724 and determine the location of mobile device 724 as a function of received signals from mobile device 724. Thomson ¶ 41. That is, when mobile device 724 "transmits one or more forged satellite measurements" based on a request sent mobile device 724 to provide navigation data message from GPS satellite 710; and circuitry (not shown) to compare (1) navigation data message assembled from signals received from GPS satellites 710 with (2)

navigation data message received from signals transmitted from mobile device 724 in order to determine whether satellite measurements transmitted from mobile device 724 have been forged. *Id.* ¶¶ 13–16, 40, 41.

The Examiner acknowledges Thomson does not teach all the claimed recitations, but instead relies on (1) Liu for teaching "comparing the untrusted location to a database of known spoofed locations" and "comparing the untrusted location with a plurality of locations" (Final Act. 4 (citing Liu ¶ 43)) and (2) Varoglu for teaching "determining the location . . . statistically overrepresent in the plurality of locations" (Final Act. 4–5 (citing Varoglu ¶ 102)).

Appellants dispute the Examiner's factual findings regarding Thomson, Liu, and Varoglu, as well as the Examiner's rationale for the combination. First, Appellants contend the cited prior art, including Thomson, does not teach or suggest [1] "'receiv[ing] a signal identifying an untrusted location associated with a mobile . . . device'" recited in claims 1 and 16. App. Br. 7–8, 13; Reply Br. 2. According to Appellants, Thomson teaches "detecting spoofed A-GNSS [assisted global navigation satellite system] signals by comparing navigation data messages received by a GPS receiver with a navigation data message received by a reference network," but

> [Thomson's] navigation data messages do not identify a location (trusted or otherwise) associated with a mobile . . . device as recited in claim 1, and therefore cannot be taken as reasonably corresponding to "receiving a signal identifying an untrusted location associated with a mobile communication device" as recited in claim 1.

App. Br. 7. According to Appellants, "navigational data messages disclosed by *Thomson* do not identify a location, untrusted or otherwise, that is associated with a mobile . . . device." Reply Br. 2.

Second, Appellants argue the cited prior art, including Liu and Varoglu, fails to teach or suggest [2] "second data source comparator module . . . to compare the untrusted location to a plurality of locations previously received by the network module to define a second match when the untrusted location is statistically overrepresented in the plurality of locations" and [3] "spoofed location detection module . . . configured to [3a] determine if the untrusted location was determined by the mobile . . . device . . . [3b] based . . . on . . . the second match" as recited in claims 1 and 16. App. Br. 8–9, 13; Reply Br. 2–3. In particular, Appellants argue Varoglu's determining of "whether a particular area has a statistically significant number of submissions indicating that the location has unreliable location data (e.g., unreliable GPS)" is not the same as the claimed "second match when the untrusted location is statistically overrepresented in the plurality of locations." App. Br. 8 (quoting Varoglu ¶ 102) (internal quotation marks omitted).

Third, Appellants argue, given Thomson's comparison of navigational data messages received from a mobile device and satellites and such navigational data messages do not represent locations associated with a mobile device, "the proposed combination would not result in a 'compar[ison] of the untrusted location to a plurality of locations,[']" and would not "determine if the untrusted location was determined by the mobile . . . device" as recited in claim 1. App. Br. 9.

In response, the Examiner takes the position that the combination of Thomson and Varoglu suggests [1] "'receiv[ing] a signal identifying an untrusted location associated with a mobile . . . device'" as recited in claim 1 because (i) Thomson's "'satellite measurements' corresponds [sic] to the untrusted location" and (ii) Varoglu's disclosure of "'location coordinates can include latitude, longitude, and the like.'" Ans. 2 (citing Thomson ¶ 41; quoting Varoglu ¶ 43) (underlining omitted). The Examiner also responds that the combination of Thomson, Liu, and Varoglu suggests [2] "'second data source comparator module'" and [3] "'spoofed location detection module'" because (i) Liu teaches the function of Appellants' claimed "second data source comparator module," i.e., "to compare the untrusted location to a plurality of locations previously received . . . to define a second match" in the context of checking an external link against a blacklist (Ans. 3 (citing Liu ¶ 42) (emphasis and internal quotation marks omitted)); and (ii) Varoglu's disclosure of "a statistically significant number of submissions indicating that the location has unreliable location data" is the same as Appellants' claimed "untrusted location . . . statistically overrepresented in the plurality of locations" as recited in claim 1 (Ans. 3 (citing Liu ¶ 42; Varoglu ¶¶ 41, 102) (internal quotation marks omitted)).

We agree with Appellants. Contrary to the Examiner's characterization, Thomson's signals received from mobile device 724, shown in Figure 7, are used at location center 721 to identify the location of mobile device 724 "when the device [724] transmits one or more forged satellite measurements" based on a request sent mobile device 724 to provide navigation data message from GPS satellite 710. Thomson ¶¶ 40–41. However, the signals received from mobile device 724 do not

themselves "identifying an untrusted location . . . associated with a mobile . . . device" as recited in Appellants' claims 1 and 16.

Likewise, Liu's external links refer to web sites or domain names and Liu's blacklist refers to a list of unsafe external links. Liu ¶¶ 3, 6. As such, Liu's disclosure of comparing an external link (i.e., domain name) against general addresses (e.g., domain names) on a blacklist or whitelist is not and cannot be considered the same as Appellants' claimed "second data source comparator module," i.e., "to compare the untrusted location to a plurality of locations previously received . . . to define a second match" as recited in claims 1 and 16.

Similarly, Varoglu teaches a GPS receiver with sensor-assisted location technology incorporated into a mobile device (shown in Figure 2) or a vehicle (shown in Figure 3) to determine its location, and in some cases, to identify areas with unreliable location data (i.e., weak GPS due to an urban canyon). Varoglu, Abstract, ¶¶ 5, 11, 41–43, Figs. 1–2. According to Varoglu, because of weak GPS in that areas from a plurality of mobile devices, "a server computer can analyze the numerous records and determine whether a particular area has a statistically significant number of submissions indicating that the location has unreliable location data (e.g., unreliable GPS)" shown in Figure 8. Varoglu ¶¶ 100–102. However, Varoglu's disclosure of whether a particular area has unreliable location data is not the same as Appellants' claimed "untrusted location . . . statistically overrepresented in the plurality of locations" as recited in claim 1. Because Thomson, Liu, and Varoglu fail to teach the disputed limitations, there is no reason for a skilled artisan to make the combination as alleged.

Based on this record, we are persuaded of Examiner error. Accordingly, we do not sustain the Examiner's obviousness rejection of independent claims 1 and 16 and their dependent claims 2–15 and 17–24.

CONCLUSION

On the record before us, we conclude Appellants have demonstrated the Examiner erred in rejecting claims 1–24 under 35 U.S.C. § 103(a).

DECISION

As such, we reverse the Examiner's rejection of claims 1–24 under 35 U.S.C. § 103.

REVERSED