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.
14/052,713	10/12/2013	Dong Liang	FORT-013900	5451

64128 7590 09/13/2019

MICHAEL A DESANCTIS
JAFFERY WATSON MENDONSA & HAMILTON LLP
7501 Village Square Drive, Ste. 206
Castle Pines, CO 80108

EXAMINER
GERGISO, TECHANE

ART UNIT	PAPER NUMBER
2494	

NOTIFICATION DATE	DELIVERY MODE
09/13/2019	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):

eofficeaction@appcoll.com
mdesanctis@hdciplaw.com
mike.desanctis@jwmhlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte DONG LIANG[1]

Appeal 2018-008741
Application 14/052,713
Technology Center 2400

Before CAROLYN D. THOMAS, JEREMY J. CURCURI, and SCOTT RAEVSKY, *Administrative Patent Judges*.

RAEVSKY, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant seeks our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 1–6, 8–17, and 19–22, all the pending claims in the present application. App. Br. 18–23 (Claims Appendix). We have jurisdiction over the appeal under 35 U.S.C. § 6(b).

We AFFIRM.

[1]Appellant identifies Fortinet, Inc. as the real party in interest (App. Br. 3).

THE CLAIMED INVENTION

Appellant's claimed invention generally relates to systems and methods for conducting correlation analysis for security events with asset attributes of a network. *See* Abstract. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method comprising:
>
> establishing an inventory list for each of a plurality of assets of a network that are managed by a security information and event management (SIEM) device, wherein the inventory list describes attributes, including hardware and software attributes, of each of the plurality of assets;
>
> maintaining a reliability value for each of the attributes, wherein the reliability value represents a relative vulnerability to attack of an asset of the plurality of assets with which the attribute is associated;
>
> obtaining, by the SEIM[2] device, a security event;
>
> calculating, by the SIEM device, a risk level of the security event based on at least a correlation of the security event with one or more asset attributes of an asset of the plurality of assets targeted by the security event by:
>
> retrieving reliability values of the one or more asset attributes from the inventory list of the targeted asset; and
>
> adjusting the risk level based on the retrieved reliability values; and
>
> when the risk level meets a predetermined or configurable threshold, then causing, by the SIEM device, the security event to be reported to an administrator of the network.

[2] SIEM is misspelled here.

REJECTIONS

The Examiner made the following rejections:

Claims 1–6, 8–17, and 19–22 stand rejected under 35 U.S.C. § 101 as directed to a judicial exception without significantly more. Ans. 3.

Claims 1–4 and 12–15 stand rejected under 35 U.S.C. § 103 as being unpatentable over Lotem (US 2013/0312101 A1, pub. Nov. 21, 2013) and Shezaf (US 2015/0213272 A1, pub. July 30, 2015). Final Act. 6.

Claims 5, 6, 8–11, 16, 17, and 19–22 stand rejected under 35 U.S.C. § 103 as being unpatentable over Lotem, Shezaf, and Choi (US 2006/0031938 A1, pub. Feb. 9, 2006). *Id.* at 10.

We review the appealed rejections for error based upon the issues identified by Appellant and in light of the arguments and evidence produced thereon. *Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential).

ANALYSIS

Rejection under § 101

I. Principles of Law

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. However, the Supreme Court has long interpreted 35 U.S.C. § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *E.g.*, *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

In determining whether a claim falls within an excluded category, we are guided by the Supreme Court's two-step framework, described in *Mayo* and *Alice*. *Id.* at 217–18 (citing *Mayo Collaborative Servs. v.*

Prometheus Labs., Inc., 566 U.S. 66, 75–77 (2012)). In accordance with that framework, we first determine what concept the claim is "directed to." *See id.* at 219 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *see also Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk.").

Concepts determined to be abstract ideas, and thus patent ineligible, include certain methods of organizing human activity, such as fundamental economic practices (*Alice*, 573 U.S. at 219–20; *Bilski*, 561 U.S. at 611); mathematical formulas (*Parker v. Flook*, 437 U.S. 584, 594–95 (1978)); and mental processes (*Gottschalk v. Benson*, 409 U.S. 63, 67–68 (1972)). Concepts determined to be patent eligible include physical and chemical processes, such as "molding rubber products" (*Diamond v. Diehr*, 450 U.S. 175, 191 (1981)); "tanning, dyeing, making water-proof cloth, vulcanizing India rubber, smelting ores" (*id.* at 183 n.7 (quoting *Corning v. Burden*, 56 U.S. 252, 267–68 (1853))); and manufacturing flour (*Benson*, 409 U.S. at 69 (citing *Cochrane v. Deener*, 94 U.S. 780, 785 (1876))).

In *Diehr*, the claim at issue recited a mathematical formula, but the Supreme Court held that "[a] claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula." *Diehr*, 450 U.S. at 187; *see also id.* at 191 ("We view respondents' claims as nothing more than a process for molding rubber products and not as an attempt to patent a mathematical formula."). Having said that, the Supreme Court also indicated that a claim "seeking patent protection for that formula in the abstract . . . is not accorded the protection

of our patent laws, . . . and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment." *Id.* (citing *Benson* and *Flook*); *see*, *e.g.*, *id.* at 187 ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.").

If the claim is "directed to" an abstract idea, we turn to the second step of the *Alice* and *Mayo* framework, where "we must examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221. "A claim that recites an abstract idea must include 'additional features' to ensure 'that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].'" *Id.* (alterations in original) (quoting *Mayo*, 566 U.S. at 77). "[M]erely requir[ing] generic computer implementation[] fail[s] to transform that abstract idea into a patent-eligible invention." *Id.*

The U.S. Patent and Trademark Office ("PTO") recently published revised guidance on the application of § 101. *See* USPTO, *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019) ("Guidance"). Under the Guidance, we first look to whether the claim recites:

> (1) any judicial exceptions, including certain groupings of abstract ideas (i.e., mathematical concepts, certain methods of organizing human activities such as a fundamental economic practice, or mental processes); and

(2) additional elements that integrate the judicial exception into a practical application (*see* MPEP §§ 2106.05(a)–(c), (e)–(h) (9th ed. Rev. 08.2017, Jan. 2018)).

Only if a claim (1) recites a judicial exception and (2) does not integrate that exception into a practical application, do we then look to whether the claim:

(3) adds a specific limitation beyond the judicial exception that is not "well-understood, routine, conventional" in the field (*see* MPEP § 2106.05(d)); or

(4) simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception.

See Guidance, 84 Fed. Reg. at 56.

II. Step 2A, Prong One (Judicial Exception)

The Examiner determines that claim 1[3] is directed to the abstract idea of "updating a risk level of a security event based on a correlation of a security event with one or more asset attributes (reliability values) stored in an inventory list, then notifying an administrator when the risk level meets a certain threshold." *See* Ans. 3–4. For the reasons set forth below, we conclude claim 1 recites a mental process, which is an abstract idea.

The Specification discloses:

> Systems and methods are described for conducting correlation analysis for security events with asset attributes of a network by a SIEM device to enable more efficient reporting. For example, reporting of duplicate security events may be

[3] Appellant argues claims 1–6, 8–17, and 19–22 as a group. *See* Reply Br. 3–9. We select independent claim 1 as representative of claims 1–6, 8–17, and 19–22. *See* 37 C.F.R. § 41.37(c)(1)(iv).

> aggregated and reporting of security events directed at the core assets may be prioritized over others.

Spec. ¶ 17. The Specification further discloses that "security devices may inspect the network activities . . . and record all or abnormal network activities in their logs." *Id.* ¶ 29.

We determine that claim 1 recites mental processes because claim 1 broadly relates to maintaining an inventory list, maintaining reliability values, obtaining a security event, calculating a risk level, and reporting the security event. Specifically, claim 1 recites "[a] method" that recites steps including: (1) "establishing an inventory list for each of a plurality of assets of a network . . ., wherein the inventory list describes attributes, including hardware and software attributes, of each of the plurality of assets," (2) "maintaining a reliability value for each of the attributes, wherein the reliability value represents a relative vulnerability to attack of an asset of the plurality of assets with which the attribute is associated," (3) "obtaining . . . a security event," (4)

> calculating . . . a risk level of the security event based on at least a correlation of the security event with one or more asset attributes of an asset of the plurality of assets targeted by the security event by:
>
> > retrieving reliability values of the one or more asset attributes from the inventory list of the targeted asset; and
> >
> > adjusting the risk level based on the retrieved reliability values,

and (5) "when the risk level meets a predetermined or configurable threshold then causing . . . the security event to be reported to an administrator of the network."

As drafted, these limitations, under their broadest reasonable interpretation, recite mental processes that can be performed in the human mind or using a pen and paper. *See, e.g.*, *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372–73 (Fed. Cir. 2011) (determining that a claim whose "steps can be performed in the human mind, or by a human using a pen and paper" is directed to an unpatentable mental process). In this case, these limitations encompass acts people can perform using their minds or pen and paper because people can perform the "establishing" step by listing an inventory on paper, the "maintaining" step by memorizing or writing down a reliability value, the "obtaining" step by looking manually at server logs to identify security events, the "calculating" step by mentally determining a risk level, and the "causing" step by verbally providing a report to an administrator.[4]

Appellant disputes that claim 1 is directed to an abstract idea, contending the Examiner fails to adequately explain how cases cited by the Examiner relate to the specific language of claim 1, including *Electric Power Group*[5] and *CyberSource*. Reply Br. 5–6; *see* Ans. 4. We do not rely

[4] Although we consider the claims as a group, we note that independent claim 12's generic computer limitations (including a "non-transitory storage device" and "one or more processors") do not change the outcome. *See, e.g.*, *Versata Dev. Grp., Inc. v. SAP Am., Inc.*, 793 F.3d 1306, 1335 (Fed. Cir. 2015) ("Courts have examined claims that required the use of a computer and still found that the underlying, patent-ineligible invention could be performed via pen and paper or in a person's mind."); *see also* Guidance, 84 Fed. Reg. at 52 n.14 ("If a claim, under its broadest reasonable interpretation, covers performance in the mind but for the recitation of generic computer components, then it is still in the mental processes category unless the claim cannot practically be performed in the mind.").

[5] *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016).

on *Electric Power Group*. With respect to *CyberSource*, Appellant contends that the Examiner failed to explain how *CyberSource*'s "obtaining and comparing intangible data" relate to the "establishing," "maintaining," and "calculating" limitations of claim 1. Reply Br. 5. Appellant further contends, "claim 1 may obtain and compare intangible data as part of its calculation and evaluation of the risk level for the security event at issue, but that does not translate to claim 1 ***as a whole*** being ***directed to*** 'obtaining and comparing intangible data.'" *Id.* at 6.

Here, we rely on *CyberSource* for the proposition that a claim whose "steps can be performed in the human mind, or by a human using a pen and paper" is directed to an unpatentable mental process. *See CyberSource*, 654 F.3d at 1372–73. Although claim 1 does not share every characteristic of the claims in *CyberSource*, many limitations of claim 1 include similar characteristics. For example, like the *CyberSource* claim's recitation of "obtaining information," claim 1 recites "obtaining . . . a security event" and "retrieving reliability values." *See id.* at 1370. These and the other limitations of claim 1 identified above recite steps that, as we explained above, can be performed in the human mind or using pen and paper. Thus, Appellant does not convince us that *CyberSource* is distinguishable.

Accordingly, for the aforementioned reasons, we agree with the Examiner that claim 1 recites a mental process, and thus, an abstract idea. *See* Guidance, 84 Fed. Reg. 52.

III. Step 2A, Prong 2 (Integration into a Practical Application)

Under the Guidance, we now must determine if additional elements in the claims integrate the judicial exception into a practical application (*see* MPEP §§ 2106.05(a)–(c), (e)–(h)).

We discern no additional element (or combination of elements) recited in Appellant's representative claim 1 that integrates the judicial exception into a practical application. *See* Guidance, 84 Fed. Reg. at 54–55 ("Prong 2"). For example, Appellant's claimed additional elements (i.e., "managed by a security information and event management (SIEM) device" and "by the SIEM device" do not: (1) improve the functioning of a computer or other technology; (2) are not applied with any particular machine (except for a generic computer); (3) do not effect a transformation of a particular article to a different state; and (4) are not applied in any meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception. *See* MPEP §§ 2106.05(a)–(c), (e)–(h). Instead, these limitations merely serve to narrow the recited abstract idea using a generic computing device, which cannot impart patent-eligibility. *See* Spec. ¶¶ 19 ("Embodiments of the present invention include various steps . . . which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps."), 80–88 (describing a generic computer of Fig. 10); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 716–17 (Fed. Cir. 2014) (determining that a general-purpose processor that merely executes the judicial exception is not a particular machine).

Appellant contends claim 1 is similar to the claims in *Enfish* because it "relates to **specific asserted improvements** in computer-related technology—the way a security information and event management (SIEM) device evaluates the risk level of a security event so as to limit security event reporting to a network administrator." Reply Br. 8 (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016)).

The claims at issue in *Enfish* were directed to a specific type of data structure, a self-referential table for a computer database, designed to improve the way a computer carries out its basic functions of storing and retrieving data. *See Enfish*, 822 F.3d at 1335–36. In rejecting a § 101 challenge, the court in *Enfish* held that "the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Id.* at 1336.

Here, Appellant does not point to anything in the claim that resembles the inventive self-referential data structure at issue in *Enfish*. Appellant also does not direct our attention to anything in the Specification to indicate that the invention provides an improvement in a computer's technical functionality. Rather, Appellant points to the Specification as describing a solution to the problem of "too many notifications being provided to a network administrator":

> When the administrator of a large computer network wants to know the status of the whole network, a SIEM device may be deployed to collect all the logs from the multiple security devices. The SIEM device may send out an alarm to the administrator when a high risk event is received. The SIEM device may also generate a report to show the status of the network, such as the number, targets and sources of attacks that

> have been captured within a certain period. However, when a large number of security devices are deployed in a network, a SIEM device may generate too many alarms in view of the many security events collected from the security devices.

Reply Br. 7–8 (quoting Spec. ¶ 3). Appellant does not persuade us that reducing a number of alarms reported to an administrator improves the functioning of a computer. To the contrary, Appellant's invention uses a generic computer "in its ordinary capacity." *See Enfish*, 822 F.3d at 1336.

Appellant also contends that in *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016), "the [Federal Circuit] emphasized '[t]he inventive concept inquiry requires more than recognizing that each claim element, by itself was [allegedly] known in the art' and held 'an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces.'" Reply. Br. 8–9. "As such," Appellant contends,

> the specific method recited by . . . claim 1, including at least the non-conventional approach of calculating the risk level of a security event is based on a correlation of the security event with one or more asset attributes of an asset targeted by the security event is significantly more than simply instructing a computer to apply the alleged abstract idea.

Id.

Claim 1 is not like the claims addressed by *Bascom*. The claims in *Bascom* recited an Internet content filtering located at an internet service provider (ISP) server and customized to each user, such that a user's received requests for Internet content are both filtered via the user's filtering scheme and insusceptible to hacking of the user's local devices. *Bascom*, 827 F.3d at 1343–45. Unlike the claims in *Bascom*, which improved

computers as tools (by improved filtering), the claims here merely use a generic computer.

Finally, Appellant contends the claims are similar to those at issue in *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014), which Appellant characterizes as having "an inventive concept in the modification of conventional mechanics behind website display to produce a dual-source integrated hybrid display." Reply Br. 9 (emphasis omitted). Appellant argues, "the conventional mechanics of an SIEM device is modified to limit the number of security events being reported to a network administrator." *Id.* But claim 1's reduction in reported security events using a generic computer differs significantly from *DDR*'s hybrid web page, and thus, Appellant's argument is unpersuasive.

For at least these reasons, we determine that claim 1 does not integrate the judicial exception into a practical application and, therefore, is directed to the recited abstract idea (e.g., mental processes).

IV. Step 2B (Inventive Concept)

Because we find that the claims are directed to an abstract idea, we next consider whether the claims include additional limitations, such that the claims amount to significantly more than the abstract idea.

The Examiner finds that the additional elements are well-understood, routine, and conventional in the field. Ans. 5. Specifically, the Examiner finds, "Appellant's specification demonstrates that SIEM devices are well-understood, routine, and conventional. . . . As described in paragraphs 0020-0022 of Appellant's specification, such a[] SIEM device is any generic hardware device or appliance." *Id.* Appellant does not dispute this finding.

Instead, Appellant asserts that "as this is the first time the Examiner has raised § 101 after having issued ***four*** Office actions, Appellant has not been provided with an opportunity to present evidence or explanation regarding whether, for example, the above-quoted 'establishing,' 'maintain[ing],' and 'calculating' limitations are 'routine and conventional.'" Reply Br. 6.

Appellant's procedural challenge is improper. The relevant rule provides:

> (a) *Content of examiner's answer*. . . .
>
> (2) **An examiner's answer may include a new ground of rejection**. . . .
>
> (b) *Appellant's response to a new ground of rejection*. If an examiner's answer contains a rejection designated as a new ground of rejection, appellant must within two months from the date of the examiner's answer exercise one of the following two options to avoid sua sponte dismissal of the appeal as to the claims subject to the new ground of rejection:
>
> (1) ***Reopen prosecution*. Request that prosecution be reopened before the primary examiner by filing a reply under § 1.111 of this title with or without amendment or submission of affidavits (§§ 1.130, 1.131 or 1.132 of this . . . title) or other Evidence**. . . . Any request that prosecution be reopened under this paragraph will be treated as a request to withdraw the appeal.
>
> (2) *Maintain appeal*. Request that the appeal be maintained by filing a reply brief as set forth in § 41.41. . . .

37 C.F.R. § 41.39 (emphasis added). As indicated by the bold-emphasized language, the Examiner permissibly included a new ground of rejection in the Answer.[6] As also indicated by the emphasized language, Appellant had

[6] Notwithstanding this provision, for future reference, we refer the Examiner to MPEP § 2103(I): "It is essential that patent applicants obtain a prompt yet

the option to reopen prosecution and submit evidence in response to the Answer's new ground of rejection. Instead, Appellant chose to maintain the appeal by filing its Reply Brief. Thus, Appellant's procedural challenge is improper.

As we explained above, the additional limitations merely narrow the recited abstract ideas using generic computer components. Accordingly, we find that there are no additional limitations that cause the claims to amount to significantly more than the abstract idea. Thus, we determine no element or combination of elements recited in claim 1 contains any "inventive concept" or adds anything "significantly more" to transform the abstract concept into a patent-eligible application.

Because Appellant's independent claim 1 is directed to a patent-ineligible abstract concept, does not include additional elements that integrate the judicial exception into a practical application, and does not recite significantly more than the abstract idea to which the claim is directed, we sustain the Examiner's rejection of claims 1–6, 8–17, and 19–22, which Appellant argues as a group, under 35 U.S.C. § 101 as being directed to non-statutory subject matter in light of *Alice*, its progeny, and the Guidance. *See supra* n.3.

---

complete examination of their applications. Under the principles of compact prosecution, each claim should be reviewed for compliance with every statutory requirement for patentability in the initial review of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, examiners should state all reasons and bases for rejecting claims in the first Office action."

Rejection under § 103

Appellant contends Lotem and Shezaf fail to teach or suggest claim 1's "calculating . . . a risk level of the security event based on at least a correlation of the security event with one or more asset attributes of an asset of the plurality of assets targeted by the security event." App. Br. 12, 14–15. Specifically, Appellant contends, "[t]he mere mention of a correlation process in ¶ [0041] of Lotem . . . and the relative imposed risk calculation described in ¶ [0087] (simply because it uses the term 'risk') is insufficient to meet the [disputed] limitation[.]" *Id.* at 14. Appellant contends,

> [n]owhere in the portions of Lotem relied upon by the Examiner or elsewhere in Lotem does there appear to be any teaching or contemplation that the particular asset attributes targeted by the security event should be taken into account during a calculation of a risk level of a security event.

Id. at 14–15 (emphasis omitted).

The Examiner finds, "Lotem discloses the simulation attack event analysis can be used for computing the exposure level of vulnerabilities and imposed risk levels for each data-item[']s assets." Ans. 10–11 (citing Lotem ¶¶ 87, 97, 100). The Examiner further finds, "Lotem discus[s]es calculating for each node or each data item a relative imposed risk, the maximum risk the node can impose on a single path. Lotem further discuses calculating a modification update to the relative imposed risk value of a particular node or data-item asset for the security event." *Id.* at 11 (citing Lotem ¶ 87).

We agree with Appellant. Lotem discloses a "correlation process" that "correlates events with the data items to determine security events." Lotem ¶ 41. Lotem separately discloses, "[t]he risk analysis can also associate attack likelihood and risk estimations with each vulnerability or attack step." *Id.* ¶ 86. However, the Examiner does not indicate how Lotem

relates the risk estimation to the correlation process, nor can we find any such relationship in Lotem. Accordingly, we agree with Appellant that

> [n]owhere in the portions of Lotem relied upon by the Examiner or elsewhere in Lotem does there appear to be any teaching or contemplation that the particular asset attributes targeted by the security event should be taken into account during a calculation of a risk level of a security event.

App. Br. 14–15 (emphasis omitted).

We note the Examiner has not relied on any of the other cited references to teach this element. We, therefore, do not sustain the Examiner's obviousness rejection of claim 1 and its corresponding dependent claims. As claim 12 recites nearly identical language to the above-limitation of claim 1, we also do not sustain the Examiner's obviousness rejection of claim 12 and its corresponding dependent claims.

With respect to obviousness, we do not reach Appellant's further allegations of error because we find the issue discussed above to be dispositive of the obviousness rejection of all the pending claims.

DECISION

We sustain the Examiner's § 101 ground of rejection of claims 1–6, 8–17, and 19–22.

We do not sustain the Examiner's § 103 ground of rejection of claims 1–6, 8–17, and 19–22.

We, therefore, affirm the Examiner's decision to reject claims 1–6, 8–17, and 19–22.

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