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.
14/104,772	12/12/2013	Philippe Teuwen	81538461US01	5316

65913 7590 09/27/2017

Intellectual Property and Licensing
NXP B.V.
411 East Plumeria Drive, MS41
SAN JOSE, CA 95134

EXAMINER	
DHRUV, DARSHAN I	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
09/27/2017	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):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte PHILIPPE TEUWEN,
PETER MARIA FRANCISCUS ROMBOUTS and FRANK MICHAUD

Appeal 2016-007327
Application 14/104,772
Technology Center 2400

Before CARL W. WHITEHEAD JR, ERIC B. CHEN and
MICHAEL M. BARRY, *Administrative Patent Judges*.

WHITEHEAD JR., *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants are appealing the Final Rejection of claims 1–16 and 18–21 under 35 U.S.C. § 134(a). Appeal Brief 5–16. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Introduction

The invention is directed to

> A method for verifying the integrity of navigation data used to produce random values for a white-box cryptography system including: receiving information from a navigation system; verifying the integrity of the received navigation information; extracting random information from the received

navigation information; and performing a white-box cryptography operation using the extracted random information.

Abstract.

Illustrative Claim (disputed limitations emphasized)

1. *A method for verifying the integrity of navigation data used to produce random values for a white-box cryptography system* comprising:

receiving received navigation information from a navigation system;

verifying an integrity of the received navigation information;

extracting random information from the received navigation information; and

performing a white-box cryptography operation using the extracted random information.

Rejections on Appeal

Claims 1–5, 7–11, 13–16, and 18–21 are rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter because the claims as a whole, considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea.[1] Final Rejection 4–5; Answer 3.

Claims 1–12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Levy (U.S. Patent Application Publication 2011/0025558 A1; published February 3, 2011), Lee (U.S. Patent Application Publication 2012/0170740 A1; published July 5, 2012), and Yang (U.S. Patent Application Publication 2011/0291880 A1; published December 1, 2011). Final Rejection 6–12.

---

[1] "Appellant is notified that Prior 35 U.S.C. § 101 rejection for dependent claims 6 and 12 has been withdrawn. These claims has specialized computers and specifies what a system can be." Answer 3.

Claims 13 and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brown (US Patent 8,787,564 B2; issued July 22, 2014) and Farrugia (US Patent Application 2014/0101458 A1; published April 10, 2014). Final Rejection 12–15.

Claims 15, 16, 20, and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brown, Farrugia, and Kaplan (US Patent Application 2014/0195576 A1; published July 10, 2014). Final Rejection 15–18.

Claims 14 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brown, Farrugia, Kaplan, and Blom (US Patent Application 2010/0195829 A1; published August 5, 2010). Final Rejection 18–21.

ANALYSIS

Rather than reiterate the arguments of Appellants and the Examiner, we refer to the Appeal Brief (filed October 12, 2015), the Reply Brief (filed July 18, 2016), the Answer (mailed June 30, 2016) and the Final Rejection (mailed July 2, 2015) for the respective details.

35 U.S.C. § 101 Rejection

The Examiner finds claims 1–5, 7–11, 13–16, and 18–21 are directed to an abstract idea – "*receiving received navigation information, verifying the integrity, extracting random information, performing a white-box cryptography operation, comparing received information, processing the received navigation information.*" Final Rejection 5. The Examiner further finds:

> The additional element(s) or combination of elements in the claim(s) other than the abstract idea per se amount(s) to no more than: recitation of a generic computer structure that serves to

> perform generic computer function that are well-understood, routine, and conventional activities previously known within the computer security industry. Viewed as a whole, these additional claim element(s) do not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself.

Final Rejection 5.

Appellants contend:

> The rejection fails to properly apply the framework set forth by Alice [*Alice Corp. Pty. Ltd. v. CLS Bank Intern.* 134 S.Ct. 2347 (2014)] for determining subject matter eligibility. Instead, the rejections simply conclusorily [sic] state that the claim language itself (or the majority thereof) constitutes an abstract idea and that the remaining portions fail to contribute "significantly more." As such, the office action effectively circumvents the required analysis and, instead, supports the rejection on conclusory statements.

Appeal Brief 3.

We find Appellants' arguments persuasive. We find the Examiner's articulated reasoning is insufficient to support a prima facie case of nonstatutory subject matter under 35 U.S.C. § 101.[2] Consequently, we

[2] The USPTO recently issued an update to its guidance on determining subject matter eligibility, further articulating the burden placed on the Examiner in supporting a rejection based on *Alice*. July 2015 Update: Subject Matter Eligibility, available at http://www.uspto.gov/ sites/ default/ files/ documents/ieg-july-2015-update.pdf (hereinafter, "July Update"). The July Update supplements the previous interim guidance published in December of 2015, (available at http://www.gpo.gov/ fdsys/ pkg/FR-2014-12-16/ pdf/2014-29414.pdf) (hereinafter, "Interim Guidance"), which explained that the currently accepted test for determining subject matter eligibility with regard to judicial exceptions under the Supreme Court precedents in *Mayo*

reverse the Examiner's nonstatutory subject matter rejection of claims 1–5, 7–11, 13–16, and 18–21.

35 U.S.C. § 103(a) Rejection – Claims 1–12

Appellants contend:

> The office action argues that it would have been obvious to incorporate the cryptography of Lee into the sat-nav [satellite navigation] system of Levy "to conceal the encryption key using white-box cryptography, thus making it impossible to decipher the encryption key." However, Levy does not disclose any cryptographic key in the first place and, as such, the proposed rationale would not have driven a person of ordinary skill in the art to make the proposed modification.

Appeal Brief 10.

The Examiner finds Levy discloses, "*[a] method for verifying the integrity of navigation data* (¶35*) used to produce random values for a white-box cryptography system*." Final Rejection 6.

Levy paragraph 35 is reproduced below:

> The invention relates also to a method for estimating an indication of integrity of the navigation system, characterized in that it uses a device according to the invention to carry out the following steps in real time in order to estimate an indication of integrity of the system with respect to location errors x that must be of very low probability.

We agree with Appellants that Levy is silent in regard to cryptography, however we do not find Appellants' arguments persuasive because a preamble is generally not accorded any patentable weight where it

---

and *Alice* is a two-step analysis: 1) the Examiner must determine what the claim is "directed to" and whether that qualifies as a judicial exception and 2) the Examiner must determine whether the claim recites anything that qualifies as "significantly more" than the judicial exception. Appeal Brief 5.

merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. *See In re Hirao*, 535 F.2d 67, 70 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150 (CCPA 1951).

Appellants further contend the Examiner's finding that "[e]ncoding is a form of an encryption which is an indication of data to be encrypted, using cryptographic operation" is "factually and technologically incorrect; *encoding is not the same as encryption* (or a 'form' thereof)." Appeal Brief 10 (citing Final Rejection 4).

The Examiner finds:

> While the examiner acknowledges the difference between encoding and encryption, the examiner submits that the teaching of Levy's transmitted satellite signal encoding is further complemented by the teaching of Lee's data encoding technique using white box cipher in order to conceal the information. In other words, the encoding technique described in the combination is equivalent to encryption.

Answer 9.

Appellants argue, "[a] person of ordinary skill in the art would have understood that 'encoding' is the process of placing a value into a special format for transmission while encryption is the translation of data into a *secret* code." Appeal Brief 10–11 (footnotes omitted).

Appellants further argue, "[e]ven assuming *arguendo* that it would have been obvious to implement cryptography in Levy to protect a cryptographic key:"

> The office action alleges that the random variable mentioned in para. [0014] constitutes the extracted random information, but fails to allege whether it would have been

> obvious to implement Lee's cryptography to use Levy's random variable. Further, it appears that any such further modification would have been completely arbitrary and based solely on the present claims (and thus premised solely on impermissible hindsight).

Appeal Brief 12.

This is unpersuasive. The Examiner specifically finds, and we agree, it would have been obvious to implement the "white box encryption" of Lee using the "random variable" information of Levy. *See* Final Action 7–8 (citing Levy ¶¶ 14, 17, 35; Lee ¶¶ 61–62, 64–66, Fig. 4) (finding the references are analogous as pertaining to "implementing integrity and confidentiality" and it would have been obvious to an ordinarily skilled artisan to combine their identified teachings "to measure integrity of the navigation data (taught by Levy) and secure data using white-box cryptography (taught by Lee)"); *see also* Answer 9–13.

Regarding hindsight, we note that "[a]ny judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made and does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper." *In re McLaughlin*, 433 F.2d 1392, 1395 (CCPA 1971). Appellants provide no persuasive evidence to show that combining the references' teachings as explained by the Examiner was "uniquely challenging or difficult for one of ordinary skill in the art." *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 419 (2007)). We are persuaded the claimed subject matter here exemplifies the principle that "[t]he combination of familiar elements according to known methods is

likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416.

Accordingly, we sustain the Examiner's obviousness rejection of independent claims 1 and 7, as well as, dependent claims 1–6 and 8–11 not separately argued. *See* Appeal Brief 13.

35 U.S.C. § 103(a) Rejections – Claims 13–16 and 18–21

Appellants contend:

> The office action correctly concedes that Brown fails to disclose the above-cited subject matter, but goes on to cite Farrugia's computation of hashes as allegedly remedying this deficiency. Farrugia, however, does not teach that the hashes are taken against *random* data.
>
> Specifically, Farrugia's hashes are used for the purpose of verifying the integrity of the white box implementation's code.

Appeal Brief 15 (citing Farrugia, paragraph 28. Appellants contend Farrugia's "[o]bject code is *not random* data and, in fact, if the hashes were taken of random data, then they would not serve their purpose of verifying the integrity of the code." Appeal Brief 16.

We do not find Appellants' arguments persuasive. Claims 13 and 18 require, "encrypting or hashing the collected random samples to produce encrypted random samples" and "encrypt or hash the collected random samples to produce encrypted random samples" respectively. Brown discloses in Figure 1 a "cryptographic secret generator module **106** can be a pseudorandom number generator module that is seeded by the output values from the entropy source system **102**." Brown, column 2, lines 21–24. Farrugia discloses in paragraph 28, "[i]t is well known how to store these hash values and check at a random instant some particular hash value Tj by recomputing it from the compiled code at the runtime of the code to verify

the code integrity by means of a match." Farrugia generates random hash samples by checking the hash values at random instances of time. We agree the Examiner's findings that it would have been obvious to one of ordinary skill in the art "to calculate an estimate of the entropy of the collected random samples (taught by Brown) and perform a white-box cryptography operation on encrypted collected random samples (taught by Farrugia)." Final Rejection 14. Consequently, we sustain the Examiner's obviousness rejection of independent claims 13 and 18, as well as, dependent claims 14–16 and 19–21 not separately argued. *See* Appeal Brief 16.

DECISION

The Examiner's rejection of claims 1–5, 7–11, 13–16, and 18–21 under 35 U.S.C. § 101 is reversed.

The Examiner's rejections of claims 1–16 and 18–21 under 35 U.S.C. § 103 are affirmed.

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). *See* 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED