UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/325,438	12/01/2008	Samuil Shmuylovich	EMC-08-268(IN1)US	1510

80167   7590   01/30/2019
Ryan, Mason & Lewis, LLP
48 South Service Road
Suite 100
Melville, NY 11747

EXAMINER
EDWARDS, LINGLAN E

ART UNIT	PAPER NUMBER
2491	

NOTIFICATION DATE	DELIVERY MODE
01/30/2019	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):

nyoffice@rml-law.com
jbr@rml-law.com

UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

Ex parte SAMUIL SHMUYLOVICH, BORIS FARIZON,
ANOOP GEORGE NINAN, ROBERT A. LINCOURT JR.,
SVETLANA PATSENKER, ALEKSANDRA A. MESSIER, MIN YIN,
EUGENIO KOROLEV, RAJESH K. GANDI, PRAMOD KULYADI PAI,
and VENKAT R. TIRUVEEDI[1]

_____

Appeal 2018-005889
Application 12/325,438[2]
Technology Center 2400

_____

Before MAHSHID D. SAADAT, ALLEN R. MacDONALD, and
JOHN P. PINKERTON, *Administrative Patent Judges.*

MacDONALD, *Administrative Patent Judge.*

DECISION ON APPEAL

_____

[1] The real party in interest is EMC IP Holding Company LLC. App. Br. 3.

[2] This application was the subject of a previous appeal, Appeal 2013-005797.

STATEMENT OF CASE

Appellants appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20. Claims 2, 3, 5, 8, 9, 11, 14, 15, 17, and 19 were cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Exemplary Claim

Exemplary claim 1 under appeal reads as follows (emphasis added):

1. A computer implemented method comprising:

receiving, by a secure container, secret information for accessing a device in a computer environment, *wherein the secret information is in a clear text form of a database query*;

generating a plurality of representations of the secret information, the plurality of representations comprising an encrypted version of the secret information and an obfuscated character string representing the secret information;

storing the generated plurality of representations of the secret information [in]³ the secure container;

encrypting the secure container;

determining a condition of a use of the secret information; and

in response to the determining the condition, providing at least one of the plurality of representations of the secure

---

³ Although Appellants' Response Under 37 C.F.R. 1.116 dated October 7, 2016 amended claim 1 to include the limitation "storing the generated plurality of representations. . . **in** the secure container" (emphasis added), Appellants' Amendment dated March 28, 2017 included a reproduction of claim 1 that omitted the word "in." We interpret claim 1 as reciting "storing the generated plurality of representations. . . **in** the secure container" (emphasis added) to avoid a rejection under 35 U.S.C. § 112, second paragraph for indefiniteness.

information from the secure container selected from a group
consisting of:

> providing, by the secured container over a secured
> network connection, the encrypted version of the secret
> information to: (i) store the secret information in a
> process memory, (ii) to transmit the secret information in
> a payload of a communications message, and (iii) to store
> the secret information in a persistent storage; and

> providing, by the secured container over a secured
> network connection, the obfuscated character string
> representing the secret information to: (i) show the secret
> information on a display, and (ii) to store the secret
> information in a data file.

App. Br. 12 (Claims Appendix).

Rejections on Appeal[4]

The Examiner rejected claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20
under 35 U.S.C. § 112, second paragraph as being indefinite for failing to
particularly point out and distinctly claim the subject matter which the
applicant regards as the invention.

The Examiner rejected claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20
under 35 U.S.C. § 103(a) as being unpatentable over Malcolm
(US 2008/0301762 A1; published Dec. 4, 2008) ("Malcolm"), Odins-Lucas
et al. (US 2006/0225137 A1; published Oct. 5, 2006) ("Odins-Lucas"), and
Plouffe, Jr. (US 2006/0235876 A1; published Oct. 19, 2006) ("Plouffe").

---

[4] The patentability of claims 4, 6, 7, 10, 12, 13, 16, 18, and 20 is not
separately argued by Appellants. *See* App. Br. 6–11. Thus, except for our
ultimate decision, claims 4, 6, 7, 10, 12, 13, 16, 18, and 20 are not discussed
further herein.

Issues on Appeal

Did the Examiner err in rejecting claim 1 as being indefinite?

Did the Examiner err in rejecting claim 1 as being obvious?

PRINCIPLES OF LAW

Indefiniteness

A claim is indefinite when it contains words or phrases whose meaning is unclear. *In re Packard*, 751 F.3d 1307, 1304 (Fed. Cir. 2014).

Obviousness

The mere existence of differences between the prior art and the claim does not establish non-obviousness. *See Dann v. Johnston*, 425 U.S. 219, 230 (1976). Instead, the relevant question is "whether the difference between the prior art and the subject matter in question is a [difference] sufficient to render the claimed subject matter unobvious to one skilled in the applicable art." *Dann*, 425 U.S. at 228 (internal quotations and citations omitted). Indeed, the Supreme Court made clear that when considering obviousness, "the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Further, one cannot show non-obviousness by attacking references individually when the rejection is based on a combination of references. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986); *see also In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

ANALYSIS

A. Section 112 Argument

The Examiner finds that the scope of "wherein the secret information is in a clear text form of a database query," as recited in claim 1 is unclear because it is not clear how a database query in a clear text form can be used for accessing a device. Final Act. 6. In the Examiner's Answer, the Examiner further finds:

> In this case, as one of ordinary skill would recognize, "secret information" as used in the computing art refers to sensitive or protected data that not known or seen or not meant to be known or seen by unauthorized entity. On the other hand, a database query is a programming language statement that is used for accessing information stored in a database, it is well defined and standardized, such as an SQL statement. *A clear text form of a defined programming language statement, is anything but a secret.* Further, while Appellant's argument appears to suggest that the secret information is a variable of a database query, *it is not what the claim recites*. In the claim, the secret information is received by "a secure container", which, in light of the specification, is a software data structure, defined as "an object that stores other objects (its elements), and that has methods for accessing its elements" (Specification, page 8, lines 13-14), i.e., *it is an object as defined in the paradigm of objected oriented programming, it is not a database, nor a device*. Thus, *it is not clear how secret information can be in a clear text form of database query received by a secure container*.

Ans. 4–5 (emphasis added).

Appellants raise the following argument in contending that the Examiner erred in rejecting claim 1 under 35 U.S.C. § 112, second paragraph:

> It is *well known in the art* that a *database query* (such as System Query Language (SQL) query), *may be used to access information from a device* (such as information from a SQL

> databased stored on a computing device). It is also ***well known***
> that ***such queries*** (e.g., SQL queries) ***include search variables***
> ***that are read by a device*** (e.g., a relational database of a device)
> to obtain a set of data that matches the query (e.g., SQL relational
> database query). And, as such, ***such a database query***, in some
> cases, ***could include credential information*** (e.g., a user
> identifier and user password, or other credentials) [that] ***may be***
> ***used to access a device in a computer environment*** as claimed.
>
> . . .
>
> Alternatively, ***assuming arguendo, that the ordinary and***
> ***customary meanings of the terms are not clear***, the Applicants
> submit that [the] specification ***provides adequate meaning for***
> ***the terms***. Applicants respectfully submit that "receiving, by a
> secure container, secret information for accessing a device in a
> computer environment, wherein the secret information is in a
> clear text form of a database query" ***is adequately described in***
> ***the specification, at least, on Figure 2, and on page 8 line 25 to***
> ***page 9 line 25***[.]

App. Br. 7–9 (Appellants' citations omitted; panel's emphasis added).

We are persuaded the Examiner erred. More specifically, we agree
with Appellants that "wherein the secret information is in a clear text form
of a database query" is adequately described in the Specification, at least, on
Figure 2, and on page 8 line 25 to page 9 line 25 of Appellants'
Specification, and thus, the aforementioned claim element is definite for the
reasons provided in Appellants' Appeal Brief. *See* App. Br. 8–9 (citing
Spec. 8:25–9:25; Fig. 2).

Accordingly, Appellants have shown the Examiner erred in rejecting
claim 1 under 35 U.S.C. § 112, second paragraph. Therefore, we do not
sustain the rejection.

B. Section 103 Argument

The Examiner finds the combination of cited references teaches or suggests all of the elements of claim 1. Final Act. 7–10. Appellants contend the combination of cited prior art references does not teach or suggest "generating a plurality of representations of the secret information, the plurality of representations comprising an encrypted version of the secret information and an obfuscated character string representing the secret information; storing the generated plurality of representations of the secret information the secure container; [and] encrypting the secure container," as recited in claim 1 because:

> The cited passages of Odins-Lucas mainly *only appears to describe how information may be copied from a source application, and pasted to a target application using a data object, . . .* but *it was never contemplated that such data object, as disclosed in Odins-Lucas, would be encrypted and stored, unlike the secure containers as claimed.* Such data objects as disclosed in Odins-Lucas, at least, at the time its filing in 2005, were stored in Random Access Memory (RAM) and were not considered for storage in a more persistent memory. Also, because of the nature of copying and pasting information from a target application to a source application by the same end-user, *there was never a need for any of the related data to be encrypted.*
>
> . . .
>
> In addition, Applicants respectfully submit that the combination [does] not describe how [the] data object as disclosed in Odins-Lucas would store the generated a plurality of representations of the secret information, which includes an encrypted version of the secret information and an obfuscated character string representing the secret information. That is, *Odins-Lucas does not teach or suggest that the clipboard and drag-and-drop objects, which copy plain text might be modified to store "an encrypted version of the secret information" as claimed.*

Further, as noted above *Odins-Lucas does not disclose encryption, including encrypted secret information in an object, or "providing at least one of the plurality of representations of the secure information from the secure container" or providing encrypted secret information in process memory, payloads of communication messages, or persistent storage.* The portions of Odins-Lucas relied upon by the Examiner merely state that an intermediate data object might include copied data in a variety of formats. *Odins-Lucas notably does not disclose or suggest providing secure information as encrypted information for use in a process memory, in a payload of a communications message, or in a persistent storage. Malcolm in view of Odins-Lucas does not cure these deficiencies and one skilled in the relevant arts would not bridge this gap.*

App. Br. 10–11 (Appellants' emphasis and citations omitted; panel's emphasis added).

In the Examiner's Answer, the Examiner further finds:

[I]n response to applicant's arguments against the references individually, *one cannot show nonobviousness by attacking references individually when the rejections are based on combinations of references.* . . . Malcolm disclosed [using] *different representations of secret information* under different conditions, and providing them via secured manner. *The difference between Malcolm and the claimed invention is how the different representations are organized and stored*, i.e., use of objected oriented programming paradigm, *which is clearly disclosed by Odins-Lucas and Plouffe.* Odins-Lucas teaches the concept of using *data objects* (i.e. containers) *to encapsulate different representations of subject data* (Odins-Lucas: par 0018, 0019, the "intermediate data object" (i.e. container) may contain and provide different formats and types of data depending on the capabilities of source application and target applications, and further par 0017, use of OLE, i.e., OLEObject provides data objects and methods for accessing corresponding data objects). While Odins-Lucas teaches a system providing a clipboard or drag-and-drop interface of a graphical computer

8

interface, a source application includes trust information along with data that is proffered to a target application. *The target application conditions its acceptance of such data based on the trust information"*, *it is not what the examiner cited for teaching the claimed limitation*. Rather, the examiner cited Odins-Lucas to teach use of *data object* for *providing different data format/representations within one data object*, in the processing and transmitting of data, in the implementation of the system for protecting content during system operations. Thus, one of ordinary skill in the art would have been capable of applying this known technical implementation (object oriented design), in the same manner to the prior art software system of Malcolm, i.e., one skilled in the art would readily recognize that by implementing a data object for encapsulating different format, the system would able to provide modularity, ease reuse of code through inheritance, flexibility through polymorphism (which are fundamental features of objected oriented design concept), and *the result would have been predictable*. Use of known technique to improve similar system in the same way provided in the teachings of prior art is part of the ordinary capabilities of one skilled in the art.

. . .

Further, Plouffe disclosed the concept of *encrypting data object container* and *providing the encrypted secure container* (Plouffe, par 0017, encrypted objected being passed from a first application to a second application), which provides a protection mechanism to data objects (i.e. containers). One of ordinary skill in the art *would have been motivated to implement the system of Malcolm with the object oriented design paradigm for data representation and encryption of data objects for transmission and storage disclosed by Plouffe in order to provide better access efficiency and protection for the application data*.

Ans. 9–10 (Examiner's citations omitted; panel's emphasis added).

We are not persuaded that the Examiner erred for the reasons articulated in the Examiner's Answer. More specifically, we agree with the Examiner that Appellants' arguments attack the references individually

rather than the combination of references, as Appellants allege that Odins-Lucas fails to teach an element of claim 1 (*i.e.*, "encrypting the secure container"), but the Examiner relies upon Plouffe rather than Odins-Lucas for teaching the aforementioned claim element. *See* Final Act. 10 (citing Plouffe ¶ 17); *see also* Ans. 10. Further, Appellants fail to provide any factual evidence in support of Appellants' contention that it was never contemplated, at the time of the filing of the Odins-Lucas reference, that the data object disclosed in Odins-Lucas would be encrypted and stored. Mere attorney arguments and conclusory statements that are unsupported by factual evidence are entitled to little probative value. *In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997).

We have considered Appellants' other arguments, and they are not persuasive either. Accordingly, Appellants have not shown the Examiner erred in rejecting claim 1 under 35 U.S.C. § 103(a).

CONCLUSIONS

(1) The Examiner erred in rejecting claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20 as being indefinite under 35 U.S.C. 112, second paragraph.

(2) The Examiner has not erred in rejecting claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20 as being unpatentable under 35 U.S.C. § 103(a).

(3) Claims 1, 6–14, 18, and 19 are not patentable.

DECISION

We reverse the Examiner's rejection of claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20 under 35 U.S.C. § 112, second paragraph.

We affirm the Examiner's rejection of claims 1, 4, 6, 7, 10, 12, 13, 16, 18, and 20 as being unpatentable under 35 U.S.C. § 103(a).

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