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.
14/542,481	11/14/2014	Dino Dai Zovi	SQR-10810;SQ-0311-US1	3033

129981 7590 12/19/2019

Mattingly & Malur, PC - Square
1800 Diagonal Road, Suite 210
Alexandria, VA 22314

EXAMINER
BEHESHTI SHIRAZI, SAYED ARESH

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
12/19/2019	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):

cbarnitz@mmiplaw.com
ptomail@mmiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte DINO DAI ZOVI

Appeal 2018-000719
Application 14/542,481
Technology Center 2400

BEFORE JUSTIN BUSCH, JAMES W. DEJMEK, and JOYCE CRAIG, *Administrative Patent Judges*.

DEJMEK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–20. We have jurisdiction over the pending claims under 35 U.S.C. § 6(b).

We reverse.

[1] Throughout this Decision, we use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42 (2016). Appellant identifies Square, Inc. as the real party in interest. Appeal Br. 3.

STATEMENT OF THE CASE

Introduction

Appellant's disclosed and claimed invention generally relates to "protecting information displayed on an end user device against attempts to capture such information." Spec. ¶ 1. More specifically, Appellant describes a scenario wherein a user's computer may be compromised (i.e., by malware). Spec. ¶ 15. According to the Specification, such a compromised computer may be vulnerable to the detection and capture of sensitive user data. Spec. ¶¶ 13–15. "[E]ven with the images encrypted, the images can still potentially be captured by malware after the images are decrypted by the recipient's computer if the recipient's computer is compromised." Spec. ¶ 13. To mitigate the risk of a decrypted image being intercepted by malware, Appellant describes loading a cryptographic shader into a graphics processor unit (GPU) of the user's computer to perform the decryption of the image. Spec. ¶ 16. In a disclosed embodiment, the GPU is separate from the computer's central processing unit (CPU). *See* Spec. ¶ 31. According to the Specification, "the likelihood of an unscrupulous party being able to intercept the decrypted image with a malware that operates on the [user's computer] is decreased, because the decrypted image data is only decrypted on the GPU and then rendered directly to the screen." Spec. ¶ 59.

Claim 1 is illustrative of the subject matter on appeal and is reproduced below with the disputed limitations emphasized in *italics*:

> 1. A method in a mobile computing device for protecting sensitive information that is to be displayed by the mobile computing device, the method comprising:
>
> *loading a cryptographic shader into a graphics processor unit (GPU) in the mobile computing device separate from a central processing unit (CPU) in the mobile computing device,*

wherein the cryptographic shader includes shading instructions that implement at least a portion of a white-box cryptographic algorithm, wherein a cryptographic key is integrated within the white-box cryptographic algorithm so that the cryptographic key is protected from extraction, and wherein the white-box cryptographic algorithm is configured to decrypt encrypted images;

receiving, at the mobile computing device, the sensitive information in the form of an encrypted image from a remote server via a wireless communication network, wherein the encrypted image has been encrypted by the remote server with the cryptographic key;

transferring, by the CPU in the mobile computing device, the encrypted image from a main memory in the mobile computing device to the GPU;

generating, by the GPU, a decrypted image by decrypting the encrypted image using the cryptographic shader loaded in the GPU; and

loading the decrypted image directly from the GPU into a frame buffer that is coupled to the GPU and associated with a display device of the mobile computing device, for display by the display device, without any portion of the decrypted image passing through the CPU or the main memory.

The Examiner's Rejections

1. Claims 1–20 stand rejected under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. Final Act. 5–6.

2. Claims 1, 4, 6–8, 12, 14–16, and 20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Goss (US 2005/0213766 A1; Sept. 29, 2005); Nelson et al. (US 2011/0225406 A1; Sept. 15, 2011)

("Nelson"); and Mikhailov et al. (US 8,850,216 B1; Sept. 30, 2014) ("Mikhailov").[2] Final Act. 7–15.

3. Claims 2, 3, 9, 10, 17, and 18 stand rejected under 35 U.S.C. § 103 as being unpatentable over Goss, Nelson, Mikhailov, and Watanabe (US 2007/0154018 A1; July 5, 2007). Final Act. 15–20.

4. Claims 5 and 13 stand rejected under 35 U.S.C. § 103 as being unpatentable over Goss, Nelson, Mikhailov, and Yoon et al. (US 2015/0039883 A1; Feb. 5, 2015) ("Yoon"). Final Act. 20–21.

5. Claims 11 and 19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Goss, Nelson, Mikhailov, Watanabe, and Yoon. Final Act. 21–22.

ANALYSIS[3]

Rejection under 35 U.S.C. § 101

Appellant disputes the Examiner's conclusion that the pending claims are directed to patent-ineligible subject matter. Appeal Br. 8–35; Reply Br. 2–11. In particular, Appellant argues that when properly considered as a whole, the claims provide an improvement in the functioning of a computing

[2] Although the statement of rejection only identifies claims 1, 4, 6–8, 12, and 14, we note that the body of the rejection further identifies claims 15, 16, and 20. *See* Final Act. 13–15. Appellant does not argue prejudice as a result of the incomplete statement of rejection. Accordingly, we treat the omission of claims 15, 16, and 20 from the statement of rejection as a harmless, typographical error.

[3] Throughout this Decision, we have considered the Appeal Brief, filed June 27, 2017 ("Appeal Br."); the Reply Brief, filed October 26, 2017 ("Reply Br."); the Examiner's Answer, mailed August 29, 2017 ("Ans."); and the Final Office Action, mailed November 18, 2016 ("Final Act."), from which this Appeal is taken.

device by preventing the unauthorized capture of decrypted images (i.e., improved security). Appeal Br. 11, 14–18 (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016)). Additionally, Appellant asserts the claims recite more than the alleged abstract idea of encrypting/decrypting sensitive data (*see* Final Act. 6) by providing for the non-conventional arrangement of elements, such as a cryptographic shader loaded into a graphics processor unit (GPU) separate from a central processing unit (CPU). Appeal Br. 19–24 (citing *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016)).

The Supreme Court's two-step framework guides our analysis of patent eligibility under 35 U.S.C. § 101. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). In addition, the Office published revised guidance for evaluating subject matter eligibility under 35 U.S.C. § 101, specifically with respect to applying the *Alice* framework. USPTO, *2019 Revised Patent Subject Matter Eligibility Guidance*, 84 Fed. Reg. 50 (Jan. 7, 2019) ("Office Guidance"). If a claim falls within one of the statutory categories of patent eligibility (i.e., a process, machine, manufacture, or composition of matter) then the first inquiry is whether the claim is directed to one of the judicially recognized exceptions (i.e., a law of nature, a natural phenomenon, or an abstract idea). *Alice*, 573 U.S. at 217. As part of this inquiry, we must "look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter." *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016). Per Office Guidance, this first inquiry has two prongs of analysis (i) does the claim recite a judicial exception (e.g., an abstract idea); and (ii) if so, is the judicial exception integrated into a

practical application. 84 Fed. Reg. at 54. Under the Office Guidance, if the judicial exception is integrated into a practical application, *see infra*, the claim is patent eligible under § 101. 84 Fed. Reg. at 54–55. If the claims are not directed to an abstract idea, the inquiry ends. *See McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016). However, if the claim *is* directed to a judicial exception (i.e., recites a judicial exception and does not integrate the exception into a practical application), the next step is to determine whether any element, or combination of elements, amounts to significantly more than the judicial exception. *See Alice*, 573 U.S. at 217; *see also* 84 Fed. Reg. at 56.

The Examiner concludes the claims are directed to "encrypting/decrypting sensitive data," which the Examiner interprets as merely "a mathematical procedure for converting one form of numerical representation to another." Final Act. 5–6 (citing *Digitech Image Techs., LLC v. Elec. for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014)). Moreover, the Examiner finds the claims do not recite significantly more than the abstract idea, and that the claims merely recite generic functions that are well-understood, routine, and conventional. Final Act. 6; Ans. 12–13. Further, in response to Appellant's assertions, the Examiner determines that the encryption/decryption of data (which is the focus of the claims) does not provide an improvement to the technology. Ans. 14.

Although we agree that the claims involve the encryption and decryption of sensitive data, we are mindful that "an invention is not rendered ineligible for patent simply because it involves an abstract concept." *Alice*, 573 U.S. at 271. As set forth in the claims, an encrypted image is received by the computing device and is transferred from a main

memory by the CPU to the GPU. *See, e.g.*, claim 1. The GPU, using a cryptographic shader, decrypts the image, and loads the decrypted image directly into a frame buffer for display. *See, e.g.*, claim 1.

Here, we conclude that the focus of the claims (i.e., the character of the claims as whole) is more than merely the encryption and decryption of sensitive data. Instead, we conclude the claims are directed to improving the security of the computing device by decrypting an encrypted image within the GPU. As provided in the Specification, by containing the decryption of the image within the GPU, "the vulnerability to malware's eavesdropping or impersonation [is reduced] because the only place where the decrypted image exists is on the GPU and not the application processor (i.e., the CPU)." Spec. ¶ 59; *see also Enfish*, 822 F.3d at 1337 (explaining the conclusion that the claims are directed to an improvement of an existing technology is bolstered by the specification's teachings).

As the court discussed in *Enfish*, claims that improve an existing technology might not succumb to the abstract idea exception of patent eligibility. *Enfish*, 822 F.3d at 1335. In *Enfish*, the court framed the first step of the *Alice* inquiry as whether the focus of the claims is on a specific asserted improvement in computer capabilities or, instead on an abstract idea that merely uses a computer as a tool for carrying out the abstract idea. *Enfish*, 822 F.3d at 1335–36. In addition, our reviewing court has also recently concluded that claims directed to improving computer security improve the functioning of the computer itself and are, therefore, patent eligible. *See SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1304 (Fed. Cir. 2019); *Ancora Tech., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1344 (Fed. Cir. 2018). As discussed above, we find that the instant claims are directed

to improving the security of a computing device. Accordingly, we conclude the claims are patent eligible under 35 U.S.C. § 101.

Moreover, analysis under the Office Guidance does not alter our conclusion. The Examiner concludes the claims are directed to an abstract idea. *See* Final Act. 5–6; Ans. 5–11. In particular, the Examiner concludes the claims are directed to encrypting/decrypting sensitive data, which is a mathematical concept (i.e., a mathematical procedure for converting one form of numerical representation to another) and, therefore an abstract idea. Ans. 5; *see also* 84 Fed. Reg. at 52; *Digitech*, 758 F.3d at 1351.[4]

Claim 1 is reproduced below and includes the following claim limitation(s) that recite encrypting/decrypting sensitive data, emphasized in *italics*:

> 1. A method in a mobile computing device for protecting sensitive information that is to be displayed by the mobile computing device, the method comprising:
>
> loading a cryptographic shader into a graphics processor unit (GPU) in the mobile computing device separate from a central processing unit (CPU) in the mobile computing device, wherein the cryptographic shader includes shading instructions that implement at least a portion of a white-box cryptographic algorithm, wherein a cryptographic key is integrated within the white-box cryptographic algorithm so that the cryptographic key is protected from extraction, and wherein the white-box cryptographic algorithm is configured to decrypt encrypted images;
>
> *receiving*, at the mobile computing device, *the sensitive information in the form of an encrypted image* from a remote server via a wireless communication network, wherein the

[4] In *Digitech*, the court circumscribed its conclusion that merely using mathematical algorithms to manipulate existing information to generate new information is not patent eligible "[*w]ithout additional limitations*." *Digitech*, 758 F.3d at 1351 (emphasis added).

> encrypted image has been encrypted by the remote server with the cryptographic key;
>
> transferring, by the CPU in the mobile computing device, the encrypted image from a main memory in the mobile computing device to the GPU;
>
> *generating*, by the GPU, *a decrypted image by decrypting the encrypted image using the cryptographic shader* loaded in the GPU; and
>
> loading the decrypted image directly from the GPU into a frame buffer that is coupled to the GPU and associated with a display device of the mobile computing device, for display by the display device, without any portion of the decrypted image passing through the CPU or the main memory.

Because the claim recites an abstract idea (i.e., generating a decrypted image by decrypting the encrypted image using the cryptographic shader), we next determine whether the claim integrates the abstract idea into a practical application. 84 Fed. Reg. at 54. To determine whether the judicial exception is integrated into a practical application, we identify whether there are "*any additional elements recited in the claim beyond the judicial exception(s)*" and evaluate those elements to determine whether they integrate the judicial exception into a recognized practical application. 84 Fed. Reg. at 54–55 (emphasis added); *see also* Manual of Patent Examining Procedure ("MPEP") § 2106.05(a)–(c), (e)–(h) (9th ed., Rev. 08.2017, Jan. 2018).

As discussed above, we find the additional limitations integrate the abstract idea (as identified by the Examiner) into a practical application—specifically improving the security (and functioning) of the computing device. *See* MPEP § 2106.05(a). In particular, the additional limitations of loading the cryptographic shader into the GPU, transferring the received

encrypted image from a main memory to the GPU by the CPU, decrypting the image within the GPU, and loading the decrypted image directly from the GPU into a frame buffer for display improve the security and functioning of the computing device by containing the decryption and decrypted image within the GPU where it is less susceptible to unauthorized capture by malware. *See* Spec. ¶ 59; *see also* MPEP § 2106.05(a).

Moreover, we find the court's holding in *BASCOM* instructive. In *BASCOM*, the court determined that although filtering Internet content is a "longstanding, well-known method of organizing human behavior, similar to concepts previously found to be abstract," the inventors had recognized "a filter implementation versatile enough that it could be adapted to many different users' preferences while also installed remotely in a single location." *BASCOM*, 827 F.3d at 1348–51. Thus, when considered as an ordered combination, the court concluded the claims provided an inventive concept "in the non-conventional and non-generic arrangement of known, conventional pieces." *BASCOM*, 827 F.3d at 1350.

The court's reasoning in *BASCOM* is applicable here. Appellant describes the "conventional notion of offloading cryptographic calculations from a CPU to a GPU." Spec. ¶ 15. However, Appellant further describes that with the conventional approach, decrypted images may be subject to capture by malware (e.g., by a malware program eavesdropping on communications between the CPU and memories by). Spec. ¶ 15. By loading a cryptographic shader in the GPU, according to Appellant, the decrypted image is constrained to the GPU (where it is then buffered for display) and is "effectively shielded from attempts to capture [the decrypted image] by any malware residing on the recipient's computer." Spec. ¶ 18.

On the record before us, the Examiner has not provided sufficient evidence or technical reasoning that it was conventional to decrypt an encrypted image using a cryptographic shader loaded into a GPU. *See Berkheimer v. HP, Inc.*, 881 F.3d 1360 (Fed. Cir. 2018). Accordingly, when considered as an ordered combination, we conclude the pending claims provide an inventive concept by the unconventional arrangement of generic components to yield a technological improvement.

For the reasons discussed *supra*, we are persuaded of Examiner error. Accordingly, we do not sustain the Examiner's rejection of claims 1–20 under 35 U.S.C. § 101.

Rejections under 35 U.S.C. § 103

In rejecting independent claims 1, 6, and 14, the Examiner finds, *inter alia*, Goss teaches a graphics processor unit (GPU) in the mobile computing device separate from a central processing unit (CPU) in the mobile device. Final Act. 7 (citing Goss, Fig. 1). Further, the Examiner finds Nelson teaches loading a cryptographic shader into a GPU. Final Act. 9 (citing Nelson ¶ 9). Additionally, the Examiner finds Mikhailov teaches a cryptographic shader including shading instructions that implement at least a portion of a white-box cryptographic algorithm. Final Act. 10–11 (citing Mikhailov, col. 4, ll. 1–15). Thus, the Examiner finds the combined teachings of Goss, Nelson, and Mikhailov teach loading a cryptographic shader into a GPU (Nelson) wherein the GPU is separate from the CPU in a mobile device (Goss) and the cryptographic shader implements a white-box cryptographic algorithm (Mikhailov).

Appellant asserts that none of the references (alone or in combination) teach a graphics processor unit (GPU). Appeal Br. 39–45; Reply Br. 12–16. As such, Appellant argues that none of the references (alone or in combination) teach loading a cryptographic shader into a GPU. Appeal Br. 39–45; Reply Br. 12–16. More specifically, Appellant argues that the Examiner erred in equating the cryptographic accelerator described in Goss, or the encryption accelerator and crypto processor described in Nelson, with the claimed GPU capable of operating the claimed cryptographic shader. Appeal Br. 39–45. Rather, Appellant asserts the accelerators of Goss and Nelson are "not able to execute a shader including shading instructions." Appeal Br. 39–41; Reply Br. 12–13.

In response, the Examiner finds that a cryptographic accelerator (as described in Goss and Nelson) performs the encryption/decryption of data and, therefore, interprets the cryptographic accelerator as the claimed GPU. Ans. 19. Further, the Examiner explains "the cryptographic accelerator is dedicated to encrypting/decrypting data, wherein data *may be* [a] video file. Examiner notes GPU is a processing unit that processes video, image, etc. Therefore the cryptographic accelerator dedicated for encrypting/decrypting video file[s] would be interpreted as [a] GPU." Ans. 19–20 (emphasis added).

To be sure, the cryptographic accelerators in Goss and Nelson are separate from the CPU and decrypt encrypted data. *See, e.g.,* Goss ¶ 22, Abstract, Fig. 1; Nelson ¶ 9, Abstract, Figs. 1, 2. However, as Appellant argues, neither Goss nor Nelson describes the cryptographic accelerator as further comprising a shader program or capability, such that the decryption and shading (as well as additional graphics processing) are performed within

the GPU. *See* Appeal Br. 39–41. Rather than a GPU, separate from the CPU, generating a decrypted image using a cryptographic shader and loading the decrypted image to a frame buffer for display, as claimed, Goss describes the cryptographic accelerator as a "hybrid cryptographic accelerator" that straddles between a Secure Execution Environment (SEE) and the rest of the System-on-a-Chip (SoC). Goss ¶ 18. Moreover, Goss describes that "the CPU mediates movement of the input data and the output data between the data and output registers and the external memory." Goss ¶ 22. Additionally, Goss describes "the streaming decrypted output data are provided to one or more insecure data output registers of the hybrid cryptographic accelerator." Goss ¶ 26. In addition, Nelson describes a cryptoprocessor and a separate encryption accelerator, each communicatively coupled to an I/O controller. Nelson ¶¶ 33, 36. Nelson generally describes the cryptoprocessor as configured to generate and maintain encryption keys and the encryption accelerator as being configured to load encryption keys and "execute multiple cryptographic functions." Nelson ¶¶ 33, 36. In addition, Nelson describes that middleware may serve as an interface between an application program and the cryptoprocessor, allowing the application to interact with the cryptoprocessor, and a device driver may serve as an interface between the application and the encryption accelerator, allowing the application and middleware to interact with the encryption accelerator. Nelson ¶ 39. Thus, we do not find Goss or Nelson (alone or in combination) teaches the claimed GPU, separate from the CPU, comprising a cryptographic shader that also directly loads the decrypted image to a frame buffer for display.

Because we find it dispositive that the Examiner has not shown by a preponderance of evidence that the cited prior art teaches or reasonably suggests the claimed GPU (i.e., comprising a cryptographic shader), we do not address other issues raised by Appellant's arguments related to these claims. *See Beloit Corp. v. Valmet Oy*, 742 F.2d 1421, 1423 (Fed. Cir. 1984) (finding an administrative agency is at liberty to reach a decision based on "a single dispositive issue").

For the reasons discussed *supra*, we are persuaded of Examiner error. Accordingly, we do not sustain the Examiner's rejection of independent claim 1. For similar reasons, we do not sustain the Examiner's rejection of independent claims 6 and 14, which recite commensurate limitations. Additionally, we do not sustain the Examiner's rejections of claims 2–5, 7–13, and 15–20, which depend directly or indirectly therefrom.

CONCLUSION

We reverse the Examiner's decision rejecting claims 1–20 under 35 U.S.C. § 101.

We reverse the Examiner's decision rejecting claims 1–20 under 35 U.S.C. § 103.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–20	101	Eligibility		1–20
1, 4, 6–8, 12, 14–16, 20	103	Goss, Nelson, Mikhailov		1, 4, 6–8, 12, 14–16, 20

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
2, 3, 9, 10, 17, 18	103	Goss, Nelson, Mikhailov, Watanabe		2, 3, 9, 10, 17, 18
5, 13	103	Goss, Nelson, Mikhailov, Yoon		5, 13
11, 19	103	Goss, Nelson, Mikhailov, Watanabe, Yoon		11, 19
Overall Outcome				1–20

REVERSED