



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.
90/014,865	09/21/2021	6411941	TO BE DETERMINED	2765
22242 7590 03/11/2022 FITCH EVEN TABIN & FLANNERY, LLP 120 SOUTH LASALLE STREET SUITE 2100 CHICAGO, IL 60603-3406			EXAMINER NGUYEN, MINH DIEU T	
			ART UNIT	PAPER NUMBER
			3992	
			MAIL DATE	DELIVERY MODE
			03/11/2022	PAPER

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.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

FITCH EVEN TABIN & FLANNERY, LLP
120 SOUTH LASALLE STREET SUITE 2100
CHICAGO, IL 60603-3406

***EX PARTE* REEXAMINATION COMMUNICATION TRANSMITTAL FORM**

REEXAMINATION CONTROL NO. 90/014,865 .

PATENT UNDER REEXAMINATION 6411941 .

ART UNIT 3992 .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	Control No. 90/014,865	Patent Under Reexamination 6411941	
	Examiner MINH DIEU T NGUYEN	Art Unit 3992	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

- a. ☒ Responsive to the communication(s) filed on 21 September 2021.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

- c. ☒ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter.
Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c)**.
If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- | | |
|--|---|
| 1. ☐ Notice of References Cited by Examiner, PTO-892. | 3. ☐ Interview Summary, PTO-474. |
| 2. ☐ Information Disclosure Statement, PTO/SB/08. | 4. ☐ _____. |

Part II SUMMARY OF ACTION

- 1a. ☒ Claims 1-3,6-14 and 16 are subject to reexamination.
- 1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☒ Claims 1-3,6-14 and 16 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
1 ☐ been received.
2 ☐ not been received.
3 ☐ been filed in Application No. _____.
4 ☐ been filed in reexamination Control No. _____.
5 ☐ been received by the International Bureau in PCT application No. _____.

* See the attached detailed Office action for a list of the certified copies not received.

9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

This non-final Office Action is in response to the communication dated 9/21/2021.

Claims 1-3, 6-14 and 16 are subject to reexamination and rejected below.

I. Procedures Governing Reexamination

Proposed Amendments, Affidavits, or Declarations

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and 37 CFR 41.33 after appeal, which will be strictly enforced.

Patent owner is notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c).

The US Patent 6,411,941 has expired, pursuant to 37 CFR 1.530(j), "[n]o amendment, other than the cancellation of claims, will be incorporated into the patent by a certificate issued after the expiration of the patent".

Extensions of Time

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extension of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

Concurrent Litigation

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the patent at issue in this reexamination proceeding throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

II. Grounds of Rejection

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of

rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1-2, 11 and 13 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hellman (US 4,658,093) and further in view of Chou et al. (US 5,892,806).

As to claim 1, Hellman discloses a method of restricting software operation within a license (*i.e., limiting use of software within authorized uses, Hellman, 9:29-10:13, 10:33-54, 10:55-65*) for use with a computer (*i.e., base unit 12, Hellman: Figs. 1, 6*) including a volatile memory area (*i.e., base unit 12 has a temporary memory 28, e.g., RAM (Random Access Memory), Hellman: Fig. 6*) and an erasable, non-volatile memory area of a BIOS of the computer (*i.e., base unit 12 has a non-volatile memory 37, which could be implemented as EEPROM, Hellman: Fig. 6*). Hellman does not explicitly disclose the computer (base unit 12) has BIOS stored in memory, Chou discloses a BIOS EEPROM 15 on a computer (*Chou: Figs, 1, 3, 7, 1:54-2:7, 3:21-35*). It would have been obvious for one of ordinary skill in the art to store both the license information and the BIOS in Hellman's erasable, non-volatile memory 37 (*e.g., EEPROM*), the method comprising the steps of:

selecting a program residing in the volatile memory (*i.e.*, *selecting software package 17 residing in temporary RAM memory 28. The software package 17 is obtained "by purchasing it at a store, over telephone line, or in some similar manner."* Hellman, 5:51-56; *selecting the software package 17 as part of generating a request for authorization, such as by extracting the software name from the software package 17, Hellman, 5:57-61; selecting the software package 17 for input to the cryptographic hash function to calculate the cryptographic hash H, Hellman, 9:15-28; selecting the software package 17 for use by the software player 42, Hellman, 10:33-65; if the software package 17 "is a computer program, then software player 42 would be a microprocessor or central processing unit (CPU)."*, Hellman, 10:66-11:3).

using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record (*i.e.*, *using update unit 36 (acting as the claimed "agent") to set up a verification structure in non-volatile memory 37, Hellman, 10:1-4. The update unit 36 sets up the claimed "verification structure" in the non-volatile memory 37 in the form of storing value M at a specific address H for a software program identified by that hash value H. The value M is the claimed "license record", because it indicates the scope of authorized use – the number of uses, where "M" is the number – for the specific software package 17 identified by hash value H, Hellman: Fig. 6. As noted above, Chou teaches storing sensitive information in the BIOS EEPROM to reduce the risk of tampering with that information, Chou, 1:54-2:7, 3:52-62, it would have been obvious to one of ordinary skill in the art to store Hellman's license information in the BIOS*

EEPROM as Chou teaches so as to discourage users from tampering the license information and to provide extra protection to the sensitive information);

verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS (*i.e., Using the value M that is stored in the non-volatile memory 37 to verify software package 17. When an attempt is made to run software package 17, the value H is generated and sent to the update unit 36, Hellman, 10:33-43. The update unit 36 uses H as an address in the non-volatile memory 37 to verify if a license exists for the software package 37. Hellman at 10:33-43. If a license does exist for the software package 17 in the non-volatile memory 37, then the update unit 36 retrieves the number of remaining authorized uses M, Hellman, 10:44-54);*

acting on the program according to the verification (*i.e., allowing the software package 17 to be used if a license record was found in the non-volatile memory 37 and there are authorized uses remaining, Hellman, 10:40-49).*

As to claim 2, the combination of Hellman and Chou discloses establishing a license authentication bureau (*i.e., An implementation of the authorization and billing unit 13 that creates an authorization A in order to securely pass license information to the base unit 12, Hellman, 6:16-7:16. Authorization A as “an authenticator which is a cryptographic function of the base unit’s key, the software, the number of times use of the software is authorized, and the random number generated by the base unit”, Hellman, 4:51-55).*

As to claim 11, the combination of Hellman and Chou discloses wherein the volatile memory is a RAM (*i.e.*, *temporary memory 28 is "for example a RAM", Hellman, 8:67-68*)

As to claim 13, the combination of Hellman and Chou discloses wherein a unique key is stored in a first non-volatile memory area of the computer (*i.e.*, *storing a serial number and a key K in the permanent memory 31, Hellman, 8:61-9:15, 9:29-32*).

2. Claims 3, 6-10, 12, 14, 16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hellman (US 4,658,093) in view of Chou et al. (US 5,892,806) and further in view of Schneck et al. (US 5,933,498).

As to claim 3, the combination of Hellman and Chou discloses wherein setting up a verification structure further comprising the steps of:

establishing, between the computer and the bureau, a two-way data-communications linkage (*i.e.*, *a two-way data communication is established between the base unit 12 and the authorization and billing unit 13 over insecure communication channel 11, Hellman, 5:39-6:8*);

transferring, from the computer to the bureau, a request-for-license including an identification of the computer and the license-record's contents from the selected program (*i.e.*, *the base unit 12 transferring a "user originated request for software use" (the claimed "request-for-license") to the authorization and billing unit 13, Hellman, 5:57-61. The request includes a "serial number, identification number, user name or similar identifier unique to base unit 12", Hellman, 5:57-65. The request also includes the*

software name identifying the software, as well as other information like the number of additional uses, N (i.e., the claimed "license record's contents from the selected program"), Hellman, 5:57-66);

forming an encrypted license-record at the bureau by encrypting parts of the request-for-license using part of the identification as an encryption key (*i.e., the billing and authorization unit 13 forming an encrypted license record in the form of authorization A, Hellman, 6:16-7:16*). Hellman discloses that the serial number could be any "identifier unique to base unit 12", Hellman, 5:59-65. Hellman does not disclose, however Schneck discloses that a public key could be used to identify a computer system (Schneck, 11:32-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to use the public key as an identifier for a computer in the system of Hellman and Chou, as Schneck teaches, to securely encrypt the authorization A.

transferring, from the bureau to the computer, the encrypted license-record (*i.e., the billing and authorization unit 13 transfers the authorization A to the base unit 12, Hellman, 6:3-15*); and

storing the encrypted license record in the erasable non-volatile memory area of the BIOS (*i.e., Hellman discloses the number of authorized uses M is stored in the non-volatile memory 37, Hellman, 9:50-10:13*). It would have been obvious to one of ordinary skill in the art to store authorization A – which includes M as a component value – at memory address H in non-volatile memory 37, instead of storing plaintext value M, to prevent a malicious actor from using the license authorization for another software package on the same base unit (because authorization A is encrypted with has

value H for the software package 17) and to prevent a malicious actor from using the license authorization on another base unit (because authorization A is encrypted with a key unique to the base unit). Schneck discloses any information stored on a non-volatile memory, as done in Hellman, should be stored in encrypted form to prevent an unauthorized use of a licensed software (Schneck, 17:6-12, 25:64-67).

As to claim 6, the combination of Hellman and Chou discloses wherein selecting a program includes the steps of: establishing a licensed-software-program in the volatile memory of the computer (*i.e., loading the software package 17 in the temporary memory 28. Schneck discloses a first step to access protected information would be to “request the operating system to read such data into memory, Schneck, 18:7-10. Once in memory, software package 17 from Hellman would be selected from the temporary memory 28, such as: by extracting the software name from the software package 17, Hellman, 5:57-61; for input to the cryptographic hash function to calculate the cryptographic hash H, Hellman, 9:15-28; or for use by the software player 42, Hellman, 10:33-65) wherein said licensed-software-program includes contents used to form the license-record (i.e., the licensed software program includes contents used to form the license record, the software package 17 is itself used to generate the hash value H, which is part of the authorization A, Hellman, 6:27-35, 6:62-66, 9:16-28).*

As to claim 7, the combination of Hellman, Chou and Schneck discloses wherein using an agent to set up the verification structure (see addressed claims 1 and 6) includes the steps of:

establishing or certifying the existence of a pseudo-unique key in a first non-volatile memory area of the computer (*i.e.*, storing a serial number and a key , K , (the claimed "pseudo-unique key") in the permanent memory 31 (the claimed "first non-volatile memory area"), Hellman, 8:61-9:15, 9:29-32); and establishing at least one license-record location in the first nonvolatile memory area or in the erasable, non-volatile memory area of the BIOS (*i.e.*, a location is established at an address associated with hash value H (the claimed "license-record location") in the non-volatile memory 37, Hellman, 9:64-10:12).

As to claim 8, the combination of Hellman, Chou and Schneck discloses wherein establishing a license-record (see addressed claim 6) includes the steps of: forming a license-record by encrypting of the contents used to form a license-record with other predetermined data contents, using the key (*i.e.*, Hellman disclosed: a "license-record" in the form of authorization A , as modified to Schneck to store authorization A in non- volatile memory 37; the "contents used to form a license-record" in the form of the software package 17 and its corresponding hash value H ; and a "key" in the form of key SK . Hellman discloses forming the authorization A by encrypting the "contents used to form a license-record ... using the key" in the form of encrypting the hash value H with other contents using the key SK (which can be the same as key K),

Hellman, 6:62-7:2, 9:29-40. Hellman discloses encrypting "other predetermined data contents" in the license record in the form of number of requested uses N and random number R , Hellman, 6:62-7:2, 9:50-63); and establishing the encrypted license-record in one of the at least one established license-record locations (i.e., storing a license record at a license-record location in the form of storing a number of authorized uses M at an address associated with hash value H in the non-volatile memory 37, Hellman 9:64-10:13).

As to claim 9, the combination of Hellman, Chou and Schneck discloses wherein verifying the program (i.e., see addressed claims 1 and 7) includes the steps of: encrypting the licensed-software-program's license-record contents from the volatile memory area or decrypting the license-record in the erasable, non-volatile memory area of the BIOS, using the pseudo-unique key (i.e. the verification could be performed would be to decrypt the authorization A using the unique key K for the based unit 12 in order to retrieve the value M included therein. The value M could then be used as already described in Hellman, Hellman, 10:33-54. One would recognize that because the authorization A was encrypted, the authorization A would have to be decrypted in order to retrieve the number of authorized uses value M); and comparing the encrypted licenses-software-program's license-record contents with the encrypted license-record in the erasable, non-volatile memory area of the BIOS, or comparing the license-software-program's license-record contents with the decrypted license-record in erasable non-volatile memory area of the BIOS (*Hellman disclosed: the "license-software-program's license-record contents" in the form of the software package 17 and*

its corresponding hash value H; the "license-record" in the form of authorization A, as modified to Schneck to store authorization A in non-volatile memory 37; and the "non-volatile memory area of the BIOS" in the form of the non-volatile memory 37, as modified by Chou to store the BIOS routines. As discussed above, when Hellman was modified by the teachings of Schneck to store authorization A in the non-volatile memory 37, it would have been obvious to decrypt the authorization A from the non-volatile memory 37 as part of verification of the software package 17. It would have been obvious to compare the decrypted authorization A with the software package 17 and the corresponding hash value H. It would be necessary to compare the hash value H included as part of the authorization A to the software package 17 that the user was attempting to use. If the base unit 12 did not perform this comparison of the hash value H in the authorization A to the hash value H for the software package 17 in use, then the tampering described above would not be prevented. As such, it would have been obvious to implement this comparison in the modified system of Hellman, and thereby include "comparing the license-software- program's license-record contents with the decrypted license-record in erasable non-volatile memory area of the BIOS."

As to claim 10, the combination of Hellman, Chou and Schneck discloses wherein acting on the program includes the step: restricting the program's operation with predetermined limitations if the comparing yields non-unity or insufficiency (*i.e.*, *restricting the software package 17 from being used if there is no license record found in the non-volatile memory 37 or there are no authorized uses left, Hellman, 10:40-54. It would have been obvious to compare the hash value H from the authorization A stored*

in the non-volatile memory 37 to the hash value H for the software package 17 that the user is attempting to use. When those hash values do not match, the authorization A does not correspond to the software package 17 that the user is attempting to use. In such a case it would have been obvious to prevent the user from using the software package 17, Hellman, 10:50-54).

As to claim 12, wherein a pseudo-unique key is stored in the non-volatile memory of the BIOS (*i.e.*, *Hellman discloses "non-volatile memory of the BIOS" in the form non-volatile memory 37, as modified by Chou to store BIOS routines. Hellman discloses that the serial number could be any "serial number, identification number, user name or similar identifier unique to base unit 12." Hellman, 5:57-6:2. Schneck discloses that "System IDs/Public keys" can be used to identify a device. Schneck 11:32-34. It would have been obvious to use a public key (the claimed "pseudo-unique key" in Hellman's system because Hellman already disclosed that a public key cryptographic system was compatible with Hellman's system, Hellman, 11:20-68. When Hellman was modified to use a public key, it would have recognized that the public key would need to be stored in the non-volatile memory 37 in order to be maintained when power was lost, Hellman, 9:16-49. Hellman only discloses two such non-volatile memories: permanent memory 31 and non-volatile memory 37. Hellman, 8:61-9:15, Figure 6. It would have been obvious to store the public key in the non-volatile memory 37 as one of a limited number of design choices, i.e., one of two options. Chou discloses that a public key can be stored in the BIOS memory, Chou, 4:6-19, Figs 3, 7. It would have been obvious to*

store the public key in the non-volatile memory 37 and to use the non-volatile memory 37 as the BIOS memory).

As to claim 14, the combination of Hellman, Chou and Schneck discloses wherein the step of using the agent to set up the verification record, including the license record, includes encrypting a license record data in the program using at least the unique key (*i.e., as discussed in claim 3, with the modification of Hellman, the authorization A is stored instead of the plaintext value M. Hellman discloses the "agent" in the form of the update unit 36 in cooperation with authorization and billing unit 13; a "verification record, including the license record" in the form of the authorization A. Schneck discloses any information stored on a non-volatile memory, as done in Hellman, should be stored in encrypted form to prevent an unauthorized use of a licensed software (Schneck, 17:6-12, 25:64-67). The software package 17 includes data used to form the authorization A. Hellman discloses that the entirety of the software package 17 is used to generate the hash value H, Hellman, 6:31-61, 9:16-28. The hash value H is part of the authorization A. Hellman, 6:62-7:2. Hellman discloses that the authorization A is encrypted using the secret key SK, which can be the same as the key K. Hellman, 6:62-7:2, 9:29-40).*

As to claim 16, the combination of Hellman, Chou and Schneck discloses wherein the step of verifying the program includes a decrypting the license record data accommodated in the erasable second non-volatile memory area of the BIOS using at

least the unique key (*i.e.*, As discussed above, Hellman discloses the “license-record” in the form of authorization A, as modified to Schneck to store authorization A in non-volatile memory 37; an “erasable, non-volatile memory area of the BIOS” in the form of the non-volatile memory 37, as modified by Chou to store the BIOS routines; and the “unique key” in the form of the key K. A person of ordinary skill in the art would have recognized that the non-volatile memory 37, an “erasable, non-volatile memory area of the BIOS” could also be an erasable second non-volatile memory area of the BIOS. When the user attempts to use the software package 17, the plaintext value M stored in the non-volatile memory 37 needs to be verified. The verification would have been performed using the authorization A. One way in which the verification could be performed would be to decrypt the authorization A using the unique key K for the base unit 12 in order to retrieve the value M included therein. The value M could then be used as already described in Hellman. Hellman, 10:33-54. A POSA would have recognized that, because the authorization A was encrypted, the authorization A would have to be decrypted in order to retrieve the number of authorized uses value M).

CORRESPONDENCE

All correspondence relating to this ex parte reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at <https://efs.uspto.gov/efile/myportal/efs-registered>

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents

United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action. Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Minh Dieu Nguyen/

Minh Dieu Nguyen
Primary Examiner
USPTO, Art Unit 3992
(571) 272-3873

Conferees:

/Ovidio Escalante/

Primary Examiner, Art Unit 3992

/M.F/

Supervisory Patent Examiner, Art Unit 3992