(51) International Patent Classification: G06F 21/60 (2013.01)

(21) International Application Number: PCT/US2015/018239

(22) International Filing Date: 2 March 2015 (02.03.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
- 61/947,111 3 March 2014 (03.03.2014) US
- 61/947,121 3 March 2014 (03.03.2014) US
- 61/947,135 3 March 2014 (03.03.2014) US
- 61/947,143 3 March 2014 (03.03.2014) US
- 61/947,152 3 March 2014 (03.03.2014) US
- 61/947,160 3 March 2014 (03.03.2014) US
- 61/947,174 3 March 2014 (03.03.2014) US
- 61/947,197 3 March 2014 (03.03.2014) US
- 61/947,206 3 March 2014 (03.03.2014) US
- 61/947,214 3 March 2014 (03.03.2014) US


(72) Inventors: TURNER, Kyle; 980 Old State Road, Binghamton, NY 13904 (US). DELANEY, Robert; 102 Westhaven Road, Ithaca, NY 14850 (US).

(74) Agents: PRICE, Frederick, JM et al; Bond, Schoeneck & King, PLLC, One Lincoln Center, Syracuse, NY 13202 (US).


(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), with international search report (Art. 21(3))

(54) Title: SYSTEM AND METHOD FOR EXTRACTING TRIGGERED DATA FROM A VARIABLE DATA STRING AND EMBEDDING THE TriggerED DATA INTO A SECURE BARCODE

200. Receive a data stream from a host computer containing at least one trigger identifying at least one portion of data to be embedded in a barcode

202. Identify each trigger in the received data stream

204. Extract each data portion identified by a trigger

206. Print a secured barcode embedded with the extracted data portions

Fig. 2

(57) Abstract: A system and method for securing a data stream containing data to be embedded in a barcode. The system comprising a printer, having a nontransitory storage medium, configured to: receive a data stream from a host computer, the data stream having at least one trigger identifying at least one portion of data to be embedded in a barcode; identify each trigger in the received data stream; extract each data portion identified by the trigger; and print a secured barcode embedded with the extracted data portions.
SYSTEM AND METHOD FOR EXTRACTING TRIGGERED DATA FROM A VARIABLE DATA STRING AND EMBEDDING THE TRIGGERED DATA INTO A SECURE BARCODE

RELATED APPLICATION DATA


FIELD OF THE INVENTION

[0002] The present invention relates to printers capable of printing security features on a media substrate and, more particularly, to a system and method for extracting triggered data from a variable data string and embedding the triggered data in secure barcode.

BACKGROUND

[0003] Security documents are used across a diverse marketplace to deter fraud, counterfeiting and theft. In most cases, the security documents are pre-printed on media. The pre-printed media must be stored in a secure location so that counterfeiters and thieves are not able to obtain the secure media which would allow them to freely print fraudulent documents.

[0004] There are printers that can print these secure patterns on demand on standard media. In brief, security printing relates to the practice of manufacturing media substrate with certain security indicia/features to prevent forgery and counterfeiting of items such as passports, checks, and prescription pads. As should be understood by those of ordinary skill in the art, security printing can include, for example, the inclusion of watermarks, UV coatings, security fibers, microprinting, holograms, phosphorescent inks, and pantographs (e.g., "void") etc. in the manufacture of the media substrate. The advantage of these "security printers" is that standard media does not have to be secured from theft as the secure documents can be created on demand.
One such security feature is a secured barcode. Some secured barcodes operate by embedding an extra layer of data within the barcode. The extra layer cannot be read by an ordinary bar code scanner. The embedded secure data on the barcode can be used to validate a secure document when it is presented for authentication, by using a particular reader programmed to read the secured barcode with the embedded secure data.

However, security printers are potential targets for counterfeiters. In particular, a counterfeiter wanting to learn the identity and other particulars of the embedded secured barcode could attempt to read the data transmitted to the printer to be encoded into the secured barcode. A counterfeiter possessing this data could potentially duplicate the complete secured barcode with embedded data and make unauthorized copies of counterfeit secured document, and would not require the specialized reader to spoof the document. Accordingly, a need exists in the art for a system and method for obscuring the data to be embedded within a barcode such that a hacker could not identify the data within a data stream sent to a printer.

SUMMARY OF THE INVENTION

The present invention recognizes that security printers capable of printer secured barcodes are targets for counterfeiters and need to be secured against someone intercepting a data stream containing data to be embedded in a secured barcode. Accordingly, various embodiments are directed to a system and method for extracting triggered data from a data stream, the trigger data obscuring the triggered data to be embedded in the secured barcode so the triggered data cannot be easily identified. Wherein the triggers embedded in the data stream identify the data to be embedded in the barcode. The triggers are intended to be unknown to a counterfeiter intercepting the data stream, and the triggers may be regularly changed and included in the data stream in various combinations and permutations so that the triggers (and thus, the triggered data) remain secret.

According to an embodiment, the system for securing a data stream containing data to be embedded in a bar code further comprises a printer, having a nontransitory storage medium, configured to: receive a data stream from a host computer, the data stream having at least one trigger identifying at least one portion of data to be embedded in a bar code; identify each trigger in the received data stream; extract each data portion identified by the trigger; and print a secured bar code embedded with the extracted data portions.
[0009] According to an embodiment, the system further comprises: a host computer, having a nontransitory storage medium, configured to: receive data identifying the trigger; and encoding the data stream having the at least one trigger.

[0010] According to an embodiment, identifying comprises: receiving data identifying the trigger; parsing the received data stream; and comparing the received data stream to the data identifying the trigger to locate any triggers within the data stream.

[0011] According to an embodiment, the data identifying the trigger is received from a second computer.

[0012] According to an embodiment, the data received from the second computer is received via a server.

[0013] According to an embodiment, extracting the data portion comprises identifying a pattern around the trigger, wherein the trigger is a reference for orienting the pattern.

[0014] According to an embodiment, the trigger comprises a code for locating the portion of data in the data stream.

[0015] According to an embodiment, extracting comprises interpreting the code of the trigger.

[0016] According to an embodiment, the at least one trigger comprises a first trigger identifying a first portion of data in the data stream, and the second trigger identifying a second, non-adjacent portion of data in the data stream.

[0017] According to another aspect, a method for securing a data stream containing data to be embedded in a bar code, comprising the steps of: receiving a data stream from a host computer, the data stream having at least one trigger identifying at least one portion of data to be embedded in a bar code; identifying each trigger in the received data stream; extracting each data portion identified by the trigger; and printing a secured bar code embedded with the extracted data portions.

[0018] According to an embodiment, the method further comprises the steps of: receiving data identifying the trigger; encoding the data stream having the at least one trigger.

[0019] According to an embodiment, the step of identifying comprises: receiving data identifying the trigger; parsing the received data stream; and comparing the received data stream to the trigger to locate any triggers within the data stream.

[0020] According to an embodiment, the data identifying the trigger is received from a second computer.
According to an embodiment, the data received from the second computer is received via a server.

According to an embodiment, the step of extracting the data portion comprises identifying a pattern around the trigger, wherein the trigger is a reference for orienting the pattern.

According to an embodiment, the trigger comprises code for locating the portion of data in the data stream.

According to an embodiment, the step of extracting comprises interpreting the code of the trigger.

According to an embodiment, at least one trigger comprises a first trigger identifying a first portion of data in the data stream, and the second trigger identifying a second, non-adjacent portion of data in the data stream.

In accordance with a preferred embodiment of the present invention, a specialized improved computer system is created - here the devices and/or systems that are specifically structured, configured, connected, and/or programmed to extract triggered data from a data stream sent from a host computer to a printer, containing data to embed into a secured barcode. This data stream encoded with triggers obscures the data to be embedded in the barcode, making it harder for counterfeiters to intercept the data and spoof the barcode.

The data transmission, communication, and any control signals between the at least one host computer and the printer are sent and received pursuant to wired or wireless communication. The wireless communication/transmission can be over a network, which can be any suitable wired or wireless network capable of transmitting communication, including but not limited to a telephone network, Internet, Intranet, local area network, Ethernet, online communication, offline communications, wireless communications and/or similar communications means. The wireless transmission can be accomplished through any wireless protocol/technology, including, but not limited to, ZigBee standards-based protocol, Bluetooth technology, and/or Wi-Fi technology. Further, this data can be encrypted as needed based on the sensitivity of the data or the location the printer, for example. The devices can be located in the same room, in a different room in the same building, and/or in a completely different building and location from each other. A user using a host computer (or a different computer) can send data transmission, control or communication signals to the printer perform any of the functionalities described herein.
BRIEF DESCRIPTION OF THE DRAWINGS

[0028] The present invention will be more fully understood and appreciated by reading the following Detailed Description in conjunction with the accompanying drawings, in which:

[0029] Fig. 1 is a system architecture diagram of a printer that is in communication with a host computer, according to an embodiment of the present invention.

[0030] Fig. 2 is a flowchart of a method according to an embodiment of the present invention.

DETAILED DESCRIPTION

[0031] The present invention will be more fully understood and appreciated by reading the following Detailed Description in conjunction with the accompanying drawings, wherein like reference numerals refer to like components.

[0032] Embodiments of a thermal printer, examples of which can be used as the printer in conjunction with embodiments of the methods and systems described herein and shown in the referenced Figures, exist and are possible. Applicant hereby incorporates by reference the embodiments of thermal printer 104 disclosed in paragraphs [0010]-[0014] and [0028]-[0031] and FIGS. 1-4 of U.S. Pat. Application Publication Number 2015/0009271, entitled "System and Method of Thermal Printing Security Features." The thermal printer can be connected, configured, programmed and/or structured to perform the functions described herein.

[0033] Embodiments of a thermal transfer printer, examples of which can be used as the printer in conjunction with embodiments of the methods and systems described herein and shown in the referenced Figures, exist and are possible. The thermal transfer printer can be connected, configured, programmed and/or structured to perform the functions described herein.

[0034] Even though thermal printers and thermal transfer printers are specifically referenced and described in certain embodiments herein, other digital printers and corresponding appropriate media substrates (e.g., thermal and standard media) are contemplated to be part of the systems and methods described herein.

[0035] Turning to Fig. 1, a system architecture diagram of a thermal printer 100 that is structured, configured, and/or programmed to print security features such as pantographs, watermarks, secured barcodes, and microprinting on a thermal media substrate (not shown), and can have various communication links to a computer 102, according to an embodiment of
the present invention is shown. A user using the computer 102 (or a different computer 102) can instruct the thermal printer 100 to print a particular pre-stored security feature (e.g., a particular pantograph loaded in memory of the thermal printer 100) on a thermal media substrate, and to merge the particular security feature with variable data.

[0036] The thermal printer 100 can include a memory 104 that can store at least one security feature and preferably, a plurality of security features, and firmware 106 that can be programmed to print the at least one security feature, and preferably, the plurality of security features on demand that are stored in the memory, and to merge the security feature(s) with variable data (such as receipt, check, or prescription data, for example, as should be understood by those of skill in the art) preferably in real time depending on the particular application. The firmware 106 and memory 104 can have wired/wireless communication connections to the computer 102. In an alternative embodiment, the security feature (such as a pantograph) can be stored, updated, etc. on the computer 102.

[0037] In exemplary embodiment, thermal printer 100 may store a trigger extracting algorithm 108 in a nontransitory storage medium, such as in firmware, or primary or secondary memory. When implemented, the trigger extracting algorithm may perform the steps shown in Fig. 2, according to an embodiment. Turning now to Fig. 2, in step 200 printer 100 receives a data stream from host computer 102 containing at least one trigger identifying at least one portion of data to be embedded in a secure barcode.

[0038] In step 202, printer 100 identifies each trigger in the received data stream. Prior to receiving the data stream, printer 100 may have received data identifying each trigger from host computer 102 or from another source, such as a through the cloud (i.e., an internet service or other application operating on a remote server or device), through an application running on a mobile device, other any other method for inputting data to a printer (including at manufacture), as will be appreciated by a person of ordinary skill in the art in conjunction with a review of this disclosure. It will also be appreciated that the data identifying the triggers need not be received prior to receiving the data stream. For example, printer 100 may receive from host computer 100 a data stream, store the received data stream and wait until printer 100 receives any necessary data identifying the triggers. Regardless of when the data identifying the triggers is received, it may be stored on printer 100 and retrieved upon receiving a data stream. Once the data stream is received, and data identifying the triggers is retrieved, the data stream can be parsed and compared to the data identifying the triggers, identifying any triggers present in the data stream. As a corollary to step 202, host computer
102 can receive any data identifying the triggers so that it may place them in the data stream appropriately.

[0039] As will be appreciated, the triggers may take on any number of forms, and function in a variety of ways. For example, the triggers may be a simple text string, forming a known word, such as "date" or "receipt." Any data following the known word may be the data to be embedded. Similarly, printer 100 may be programmed to take a known set of bits, following the trigger, as the data to extract (or characters, numbers, etc.). For example, printer 100 may be programmed to extract the first 8000 bits of data following a known trigger word. Printer 100 may be further programmed to extract a number of bits occupying predetermined locations around the trigger. For example, printer 100 may be programmed to extract the data immediately preceding the trigger or ten bits after the trigger, or any pattern of bits surrounding the trigger, with the trigger serving as a reference point with which to orient the pattern.

[0040] Alternately, the trigger may itself be code identifying a portion or set of portions of the data stream to extract. For example, a trigger may read, "tr-80-60," first identifying the trigger as "tr," followed by a code which could be interpreted to identify the data to extract as the "60" characters appearing "80" characters into the bit stream. It will be appreciated that the trigger may take on any number of forms to identify any number of characters (bits, numbers, etc.) within a data stream. Furthermore, multiple triggers may be used, each identifying separate, non-adjacent portions of a data stream to extract. The triggers may also provide instructions on how to assemble the extracted data in the proper order. This may be particularly advantageous where the triggers identify multiple non-adjacent portions of data, as the non-adjacent portions may not be coded in order and may need to be reordered.

[0041] In addition, printer 100 may be programmed to identify different kinds of triggers. For example, printer 100 could be programmed to identify a trigger that serves as a simple marker of the data to be extracted, and identify another, more complex trigger, identifying the specific data to extract and how to assemble the data. Furthermore, printer 100 may be configured to identify multiple kinds of triggers within the same data stream. Using multiple kinds of triggers may be useful to prevent someone from identifying the triggers being used in any particular data stream.

[0042] A trigger may also identify a portion of code to be received in a later-sent data stream. For example, a trigger may identify the third consecutive data stream sent from computer 100 as a data stream containing the data to extract. Alternately, a trigger may
identify a set of data to extract from any data stream received during a certain interval of
time. For example, a trigger may identify a portion of data to extract from any data stream
received more than 15 seconds but less than 30 seconds after receiving the data stream
containing the trigger. In this way, the triggers may serve as a way to program printer 100 to
identify certain portions of data received at later times.

As will be appreciated, the triggers may be changed or otherwise altered in real time. Alternately different triggers may be programmed to be adopted at different times or at predetermined intervals. For example host computer, and printer could be programmed to adopt (transmit, receive and/or utilize, respectively) one set of triggers during a first time interval, and a second set of triggers during a different interval.

Once the triggers have been identified, the portion of data identified by the triggers is extracted in step 204. This step may include executing the steps preprogrammed into printer 100, or coded by the triggers or by the triggered data, or a combination of preprogrammed steps and steps coded by the triggers or triggered data, according to the various embodiments. The data may be formed from a known data type, such as characters and strings defined by a character set such as ASCII, or may be formed from a proprietary data designed specifically for encoding secured bar codes. As will be appreciated, the data may take any form sufficient for encoding a secured bar code. The extracted data may be temporarily stored in an array in primary memory, or may be stored in secondary memory to be retrieved at a later time.

In step 206, printer 100 prints a secure bar code embedded with the extracted data portions, as should be appreciated by a person of ordinary skill in conjunction with a review of this disclosure.

A reader application may be set up on a remote mobile device such as a phone or scanner connected to a cloud application, or network of host computers. The reader may be used to validate a secure barcode when it is presented for authentication. The reader can send the secure data read from the secure layer of the barcode to the cloud app or host computer network for authentication.

A "module," as may be used herein, can include, among other things, the identification of specific functionality represented by specific computer 102 software code of a software program. A software program may contain code representing one or more modules, and the code representing a particular module can be represented by consecutive or non-consecutive lines of code.
As will be appreciated by one skilled in the art, aspects of the present invention may be embodied/implemented as a computer system, method or computer program product. The computer program product can have a computer processor or neural network, for example, that carries out the instructions of a computer program. Accordingly, aspects of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment, and entirely firmware embodiment, or an embodiment combining software/firmware and hardware aspects that may all generally be referred to herein as a "circuit," "module," "system," or an "engine." Furthermore, aspects of the present invention may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction performance system, apparatus, or device.

The program code may perform entirely on the user's computer, partly on the user's computer, completely or partly on the thermal printer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

The flowcharts/block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods, and computer program products according to various embodiments of the present invention. In this regard,
each block in the flowcharts/block diagrams may represent a module, segment, or portion of code, which comprises instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be performed substantially concurrently, or the blocks may sometimes be performed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0052] While several embodiments of the invention have been discussed, it will be appreciated by those skilled in the art that various modifications and variations of the present invention are possible. Such modifications do not depart from the spirit and scope of the present invention.
What is claimed is:

1. A system for securing a data stream containing data to be embedded in a bar code, comprising:
   a printer, having a nontransitory storage medium, configured to:
   receive a data stream from a host computer, the data stream having at least one trigger identifying at least one portion of data to be embedded in a bar code;
   identify each trigger in the received data stream;
   extract each data portion identified by the trigger; and
   print a secured bar code embedded with the extracted data portions.

2. The system of claim 1, further comprising:
   a host computer, having a nontransitory storage medium, configured to:
   receive data identifying the trigger; and
   encoding the data stream having the at least one trigger.

3. The system of claim 1, wherein the configuration to identify further comprises a configuration to:
   receive data identifying the trigger;
   parse the received data stream; and
   compare the received data stream to the data identifying the trigger to locate any triggers within the data stream.

4. The system of claim 3, wherein the data identifying the trigger is received from a second computer.

5. The system of claim 4, wherein the data received from the second computer is received via a server.

6. The system of claim 1, wherein extracting the data portion comprises identifying a pattern around the trigger, wherein the trigger is a reference for orienting the pattern.

7. The system of claim 1, wherein the trigger comprises a code for locating the portion of data in the data stream.

8. The system of claim 7, wherein the configuration to extract further comprises a configuration to interpret the code of the trigger and locate the data in the data stream.

9. The system of claim 1, wherein the at least one trigger comprises a first trigger identifying a first portion of data in the data stream, and a second trigger identifying a second, non-adjacent portion of data in the data stream.
10. A method for securing a data stream containing data to be embedded in a bar code, comprising the steps of:

   receiving a data stream from a host computer, the data stream having at least one trigger identifying at least one portion of data to be embedded in a bar code;
   identifying each trigger in the received data stream;
   extracting each data portion identified by the trigger; and
   printing a secured bar code embedded with the extracted data portions.

11. The method of claim 10, further comprising the steps of:

   receiving data identifying the trigger;
   encoding the data stream having the at least one trigger.

12. The method of claim 10, wherein the step of identifying comprises:

   receiving data identifying the trigger;
   parsing the received data stream; and
   comparing the received data stream to the data identifying the trigger to locate any triggers within the data stream.

13. The method of claim 12, wherein the data identifying the trigger is received from a second computer.

14. The method of claim 13, wherein the data received from the second computer is received via a server.

15. The method of claim 10, wherein the step of extracting the data portion further comprises identifying a pattern around the trigger, wherein the trigger is a reference for orienting the pattern.

16. The method of claim 10, wherein the trigger is a code for locating the portion of data in the data stream.

17. The method of claim 16, wherein the step of extracting further comprises interpreting the code of the trigger.

18. The method of claim 10, wherein the at least one trigger comprises a first trigger identifying a first portion of data in the data stream, and a second trigger identifying a second, non-adjacent portion of data in the data stream.
Host Computer 102

Primary Memory 112

Trigger Embedding Algorithm 110

Printer 100

Memory 104

Trigger Extracting Algorithm 108

Firmware 106

Fig. 1
200. Receive a data stream from a host computer containing at least one trigger identifying at least one portion of data to be embedded in a bar code

202. Identify each trigger in the received data stream

204. Extract each data portion identified by a trigger

206. Print a secured bar code embedded with the extracted data portions
INTERNATIONAL SEARCH REPORT

PCT/US2015/018239

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 6 540 142 B1 (ALLESHOUSE BRUCE N [US]) 1 April 2003 (2003-04-01) col umn 2, line 60 - col umn 21, line 36 figures 1,5 ----</td>
<td>1-18</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

**A** document defining the general state of the art which is not considered to be of particular relevance
**B** earlier application or patent but published or after the international filing date
**L** document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
**O** document referring to an oral disclosure, use, exhibition or other means
**P** document published prior to the international filing date but later than the priority date claimed

*"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

*X* document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

*Y* document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

*"A" document member of the same patent family

Date of the actual completion of the international search
21 May 2015

Date of mailing of the international search report
01/06/2015

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016

Authorized officer
Segura, Gustavo

Form PCT/ISA/210 (second sheet) (April 2005)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>BR 0215034 A</td>
<td>03-11-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2467789 A</td>
<td>26-06-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1605081 A</td>
<td>06-04-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1456790 A</td>
<td>15-09-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2282270 A2</td>
<td>09-02-2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4161314 B2</td>
<td>08-10-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2005513627 A</td>
<td>12-05-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20040063000 A</td>
<td>09-07-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MX PA04005656 A</td>
<td>19-04-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NZ 533478 A</td>
<td>29-04-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6540142 Bl</td>
<td>01-04-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003136841 A</td>
<td>24-07-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wo 03052658 A</td>
<td>26-06-2003</td>
</tr>
</tbody>
</table>