(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 November 2018 (08.11.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/204319 A1

(51) International Patent Classification:
A61J 3/00 (2006.01) *G06K 9/18* (2006.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/US2018/030383

(22) International Filing Date:
01 May 2018 (01.05.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/492,521 01 May 2017 (01.05.2017) US

(71) Applicant: **I-PROPERTY HOLDING CORP.** [US/US]; 5121 Creekside Trail, Sarasota, FL 34243 (US).

(72) Inventors: **GERING, Thomas**; 5121 Creekside Trail, Sarasota, FL 34243 (US). **STUCK, Alexander**; Neustrasse 68, 5430 Wettingen (CH).

(74) Agent: **FITZGERALD, David, A., II** et al.; Wood Herron & Evans LLP, 441 Vine Street, Suite 2700, Cincinnati, OH 45202-2917 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2018/204319 A1

(54) Title: AUTHENTICATION SYSTEM FOR USE WITH PHARMACEUTICALS

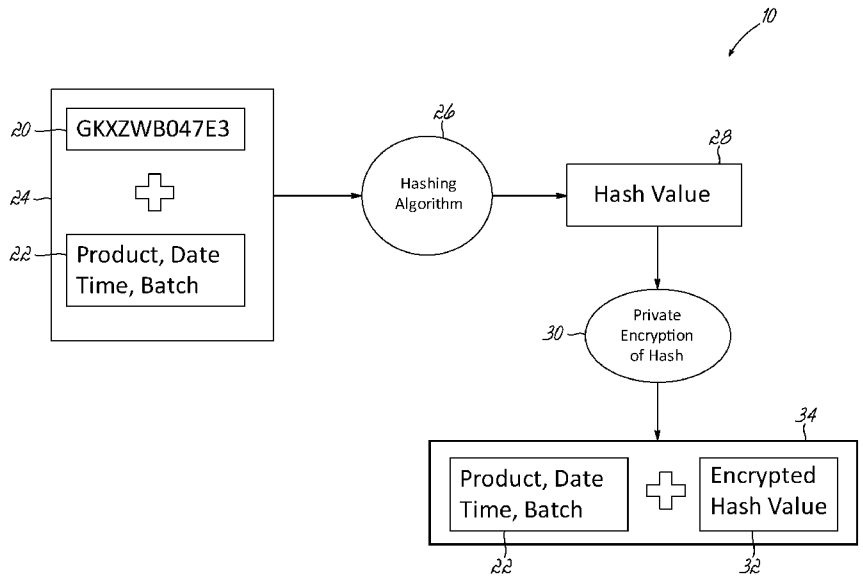


FIG. 1

(57) Abstract: An authentication system reads at random or in a predetermined sequence a few, typically 3 to 5, unique product identifiers inside the package (24) to decide whether the content is authentic or not. This cross-referencing check does not require a database connection to a central repository or database. The unique product identifiers are produced when pharmaceutical products are manufactured using embossing, for example, and a product sequence (20) is defined by physical attributes and locations of pharmaceutical products in the packaging (24), the product sequence (20) then being encrypted and used to mark the packaging (24) of the one or more packaging levels with a coding. The coding is used to authenticate the products in the packaging downstream in the supply chain.

[Continued on next page]

(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).

Published:

— *with international search report (Art. 21(3))*

AUTHENTICATION SYSTEM FOR USE WITH PHARMACEUTICALS

Cross Reference to Related Applications

[0001] This application claims priority to U.S. Provisional Patent Application Number 62/492,521, filed May 1, 2017. The above-mentioned patent application is incorporated herein by reference in its entirety.

Technical Field

[0002] This disclosure relates to the tracking and authentication of products such as pharmaceutical tablets and other elements stored in blisters or similar packaging, to verify the authenticity thereof.

Background

[0003] This application is building on earlier inventions and patent applications by the original named Applicant. These earlier applications and patents include U.S. Patent Publication No. 2015/0183257 to Glendenning et al.; International PCT Patent Publication No. WO 2016/172503 to Stuck; International PCT Patent Publication No. WO 2012/011968 to Stuck et al.; International PCT Patent Publication No. WO 2015/103396 to Glendenning et al.; U.S. Patent Publication No. 2014/0255482 to Klocke et al.; and U.S. Patent No. 8,715,725 to Stuck et al., the entire disclosures of which are hereby incorporated by reference herein in their entireties.

[0004] Pharmaceuticals and cosmetics are high-technology products which require very specialized material systems and production procedures as well as very large investments in development and marketing. Because of public safety concerns, authorities place very stringent requirements on the verification and authenticity of such products. Companies therefore have to make huge investments in the tracking and tracing of these products to ensure authenticity. In addition, as these products usually have large sales margins and are distributed globally, it is not surprising that cosmetics manufacturers and pharmaceutical companies suffer from enormous losses due to counterfeiting. The problem has been aggravated by strongly increased sales over the internet, where everything from counterfeit Viagra to false glucose tests is readily available. Furthermore, local and regional regulations are becoming more stringent regarding the authentication process required for distribution of products including pharmaceuticals.

[0005] Various governments around the world have taken the initiative in terms of efforts to increase the authenticity of pharmaceutical products in the supply chain. An overview to these various initiatives is provided at: https://www.infosys.com/SAP/collaterals/Documents/pharmaceutical-serialization-guide-to-country-wise.pdf for example. These initiatives can largely be summarized by the term "serialization" in that most of them thrive to put some sort of barcode on the secondary pharmaceutical package (mostly carton boxes) in the supply chain, and having centralized databases function as code repositories that can be called upon in order to "verify" individual packages. For various reasons these serialization attempts fall short of even achieving a reasonable level of authentication certainty, as is well known in the trade.

[0006] Track- and-trace features in the pharmaceuticals market have so far been applied to packaging in various forms. For example, holograms, optically variable inks, fluorescent dyes, and other identification features are attached to the packages, e.g., by adhesive tags. Alternatively, such labels are laminated to the carton or are directly applied to the packages. The main drawback of such labels is that they are not an integral part of the tablet and therefore do not provide 100% security. For example, if the authentic product is separated from the package, the package can be refilled with a false product.

[0007] Therefore, a primary concern is still the verification of tablets as such, and ensuring that authentic tablets in fact remain in their correct primary packaging, e.g. in the blister into which these were originally filled on the packaging line.

[0008] Once this has been ascertained, such primary packaging (blisters) containing authentic tablets should be verified as resting in the correct secondary packaging (typically carton boxes) into which those blisters have been packed originally on the packaging line.

[0009] Most governments today only require that secondary and tertiary packaging contains machine readable codes, such as datamatrix codes, which are unique for each package and serve to identify the package along the supply chain (these methods used are typically being identified by the term "serialization", as described above).

[0010] Usually, all such serialization coding has to be stored in central repositories, where a unique package code and all codes on packages within a certain outer package (sub-packages of a larger shipment) are linked and centrally stored and aggregated. This coding then creates a so-called parent-child relationship between different packaging levels. Every time a package is opened, this event should be communicated to the central repository and the

unique package code of the individual package that is being opened is invalidated. This step is usually called de-aggregation.

[0011] If the sub-packages are then again put into other packages (which often happens in the case of re-packaging by legitimate distributors along the supply chain), a new package code with a new parent/child relationship is generated and stored in the central repository (aggregation). As pharmaceuticals along the supply chain often change hands from producers to wholesalers, to distributors and finally to pharmacies, aggregation and de-aggregation can happen at many places, and at many different locations in different jurisdictions, requiring each time a package is changed to generate new coding and to invalidate the codes previously printed on the packaging.

[0012] In order not to impair the flow of goods by serialization, wholesalers are, in many jurisdictions, only required to check if a given code on the outside of a given package is actually valid. If there is no evidence of tampering with the particular package, it is then assumed that all its contents are acceptable. During de-aggregation however, often all internal packaging codes are checked against the database. No effective and efficient product authentication is required by local governmental authorities in most cases in these current supply chain scenarios. This circumstance is opening the door for counterfeiters, who can copy printed product codes and sell the corresponding packages which they manufacture using fake product, if the fake package is sold and read out against the central database before the one provided by the legitimate manufacturer is sold at a pharmacy. Effectively, this system creates a lottery that sees criminal counterfeiters winning in many cases; and even if the fake product comes up for sale too late, it is often just discarded, often with no direct and detrimental legal consequences to the counterfeiters.

[0013] Thus, it would be desirable to improve the authentication system and processes used with packaged goods such as pharmaceuticals.

Summary

[0014] With the present invention, a true authentication system is provided across the entire pharmaceutical supply chain based on physical authentication of the pharmaceutical product by use of truly random coding which serves as a basis for all codes during aggregation and any de-aggregation process along the supply chain. At any given point this inventive scheme allows to authenticate any given package and the sub-packages contained within without the need to access any external database and with a pre-determined level of

authentication confidence. In combination with state-of-the-art blockchain theory known to skilled artisans, the authentication system forms random code-based data blocks and uses those blocks as the basis for a blockchain functionality along a manufacturer's supply chain.

[0015] Applicant's inventive system is based on the fact that during pharmaceutical production most products, such as tablets and capsules, undergo a true randomization process, as they are processed in industrial tumblers and coated in large quantities in subsequent coating stations. If small variations and subgroups of these products, such as, but not limited to tablets, can be identified and distinguished from each other in production, then the distribution of these subgroups within a given primary package (such as a blister or also a tablet bottle and the like) is a true random number which does not change along the individual package's path through the supply chain. This true random number combined with overt information can then be printed on the primary and secondary package (i.e. the blister or tablet bottle or the paper box which holds blisters for sale). The number can be either directly printed or more likely crypto-graphically secured on the primary and secondary package. Whatever the coding sequence, the result is still a true random number, which is linked to the physical content of the package and can be physically authenticated.

[0016] In one embodiment of the invention, a blister contains 15 tablets in a given sequence and 3 of these blisters are packed together in a secondary package onto which a barcode is printed on the outer side. Each blister may (but does not have to) contain a printed, laser formed or embossed code that stores the information about its particular tablet sequence. In the case of embossing or laser forming, this would preferably be done at the bottom of the blister in the region where often the manufacturing or batch numbers are embossed. If a security hologram or other optical contrast mechanism is embossed into the same region, the printed, laser formed, or embossed code is visible to conventional camera equipment such as the cameras integrated into smart phones. If the blister is authenticated, using self-authentication (reading the tablet sequence of the blister with a 2D camera and checking it against the embossed, printed or laser formed code on the blister) this inventive solution has the advantage that it only requires taking one single photograph for self-authentication, i.e., the photo will identify the physical tablet sequence and simultaneously the printed/embossed/laser-formed code and a comparison is being made immediately. It is not necessary to turn the blister and read the printed code on the backside in such an authentication according to one embodiment.

[0017] In any case, however, the printed code on the outside (secondary) package may contain all information about the individual tablet positions in the blisters contained therein. To authenticate the tablets with a given statistical certainty, in some embodiments it can be sufficient to identify the correct positions of a subset of tablets within a blister and the secondary package.

[0018] In one embodiment of this invention, a secondary package contains 3 blisters of the same medication and each of the blisters has 10 tablets packed into it, and there are 2 distinguishable tablet types (for example each tablet has 2 different sides, one containing a logo and one not). An image of a blister is taken with a camera (for example a smartphone), and the sequence of tablets in this particular blister is identified. In order to reach a given level of authentication confidence it is actually not necessary that the entire sequence of the photograph matches the entire sequence of this blister as recorded on the secondary package, a subset of matches is sufficient for reliable authentication. Statistics says that if 6 out of the 10 tablets sit at the correct location with the correct orientation (up versus down) in the blister, the probability that the blister is authentic is higher than 99.9%. The inventive authentication system thus is quite stable in terms of errors or disturbances, as these might occur during transport or because of unstable image recognition by the smartphone camera/software.

[0019] If even higher authentication levels or confidence is required in the 3 blister and secondary packaging case described above, one can take a second blister and authenticate it in the same way. The probability, or in authentication, certainty (again with only 6 out of 10 tablets being correctly identified), that the package is not authentic is the square of the first probability, i.e. less than 1 in 1,000,000, with 3 blisters authenticated against the secondary package the certainty is 1 in 1,000,000,000.

[0020] The same principle also applies to bottled tablets. The difference here is that there is no order in which the tablets are arranged. By actively embossing measurable geometrical differences in the tablets and manufacturing many different types for the same tablet (for example by embossing a bar code onto the tablet as shown in applicant's U.S. Patent Publication No. 2011/0188051), it is again sufficient to take out and measure 5 tablets and reach confidence levels of 99% or more that the bottle and its content are actually authentic.

[0021] In most embodiments according to this invention, the relationships between the printed/laser-formed/embossed tablet sequence and the physical content will not be printed in

an overt manner, but crypto-graphically secured, thereby providing an additional protective layer.

[0022] The authentication system provides for stable authentication at pre-defined statistical certainty levels for tablets and the associated primary and secondary packaging. The authentication is based on truly random coding and allows authentication of a product with a predetermined and high accuracy. With the system and process relying on truly random input information and the information being crypto-graphically secured, it is in fact extremely difficult to successfully counterfeit.

[0023] To realize the inventive authentication system in a manufacturer's supply chain, the following inventive products need to be used and integrated into the system. First, certain marking of products such as pharmaceutical dosage forms needs to occur by embossing or the like, as set forth in the prior applications referenced above. Second, certain digital camera technology that can read random coding must be provided on the packaging line, as and when tablets are being packaged. For example, readers such as pOCT or time-of-flight camera technology can be used to help achieve the authentication system of this invention. Third, software applications and products that function as shown in flowcharts described below with reference to FIGS. 1 through 3 must be provided, which are implemented in customer reader or smart phone applications and which can be used for cross-referencing along the supply chain.

[0024] In all embodiments, the secondary package (i.e. smallest saleable unit in many markets around the world) is aggregated into a larger box and this box is also provided with a unique identifier, which may be used in yet further embodiments of the authentication system of this invention.

[0025] In one specific embodiment of the invention, an authentication system for pharmaceutical products includes product manufacturing equipment that uses embossing technology to form and mark the pharmaceutical products with a coding. The system also includes a packaging line that places the pharmaceutical products in one or more packaging defining one or more packaging levels. In-line reading equipment determines a product sequence defined by physical attributes and locations of pharmaceutical products in the packaging, the product sequence then being encrypted and used to mark the packaging of the one or more packaging levels with a coding. The system further includes scanning equipment at a point in a supply chain downstream from the packaging line, the scanning equipment including a camera that images the codings of the pharmaceutical products and of

the one or more packaging levels and a processor that compares the codings to one another to authenticate whether the pharmaceutical products are genuine. The product manufacturing equipment marks the pharmaceutical products without adding marking products such as inks to the pharmaceutical products. The encryption of the product sequence is achieved using public-private key. The authentication of whether the pharmaceutical products are genuine is achieved without causing the scanning equipment to communicate with a central data repository away from the supply chain.

Brief Description of the Drawings

[0026] Various additional features and advantages of the invention will become more apparent to those of ordinary skill in the art upon review of the following detailed description of one or more illustrative embodiments taken in conjunction with the accompanying drawings. The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate one or more embodiments of the invention and, together with the general description given above and the detailed description given below, serve to explain the one or more embodiments of the invention.

[0027] FIG. 1 is a schematic flow chart showing a series of steps for production and aggregation of an encrypted hash, which may be implemented by a computer having a processor and similar equipment loaded with software, in accordance with one embodiment of the present invention.

[0028] FIG. 2 is a schematic flow chart showing a series of steps for authentication and verification of a sequence using an encrypted hash, which may be implemented by a computer having a processor and similar equipment loaded with software, in accordance with one embodiment of the present invention.

[0029] FIG. 3 is a schematic flow chart showing a series of steps for authentication using symmetrical encryption, which may be implemented by a computer having a processor and similar equipment loaded with software, in accordance with one embodiment of the present invention.

Detailed Description

[0030] In accordance with one embodiment, the authentication system operates along the supply chain in the following manner.

[0031] Instead of only checking if the latest outside code is valid and included in a central database repository, as is typical in conventional systems, the authentication system reads at random or in a predetermined sequence a few, typically 3 to 5, unique product identifiers inside the package to decide whether the content is authentic or not. Again, this cross-referencing check does not require a database connection to the central repository and it can therefore be performed with relatively simple readers or smart phone software applications anywhere in the world while achieving security levels that are actually higher than the ones achievable by use of central repositories – as their sub-systems are having to deal with their own error events (readers not working reliably, database errors, aggregation errors, internet connection problems, etc.). In many of those events the central repository systems have no other choice but to send product back to the manufacturer as it cannot be reliably authenticated when in the supply chain. The authentication system of this invention eliminates such issues, as any package in the supply chain is inherently secure and can be reliably authenticated when it is already in the supply chain without the need of going back to the central repository for any information.

[0032] The authentication system is hierarchic and can be extended to any level of packaging. A user always checks the code on the outer package and compares it with a small statistically-significant sample of the codes within to reach a desired level of authentication. In terms of information every package forms a block, which is cryptographically secured and some or all packages on the same level together with their printed (or naturally measurable) codes form a blockchain, which if packaged together in a larger box itself then forms a secured block on the next higher packaging level. This inventive system fully circumvents the problem of aggregation/de-aggregation, as for de-aggregation now only the codes of the outer packages must be destroyed, while aggregation now always happens the same way by creating a secured block. The specifics of how each block is cryptographically secured can vary widely based on the embodiment, as will be readily understood by those skilled in the art. As at the lowest level (the product or blister) the product code is random and linked to the unique physical properties of an individual product, the product itself can not only be tracked and traced by the system through the supply chain from manufacture to point of distribution, but also effectively authenticated with a high degree of confidence.

[0033] In one embodiment of the invention, coding created by the authentication system is cryptographically linked to the central repository coding, which will nevertheless be necessary because of governmental requirements in target markets. However, the benefits of

reliable authentication at any point in the supply chain are still realized in such circumstances.

[0034] In the field, if there is any suspicion that a package or some barcodes have been tampered with, when using the authentication system, it is possible to go down to any packaging level deemed necessary reading aggregated coding to evaluate authenticity of the product. In the authentication system such reading of aggregated coding on various packaging levels can even go down to the product level and thereby authenticate the contents of any package. Therefore, the hierarchical authentication system of this invention is almost entirely immune against simple copying of some or all barcodes on the packages by counterfeiters, which is deemed the most probable attack scenario based on currently-known counterfeit activity.

[0035] This approach of scanning the contents of a package also implicitly provides tamper evidence at the same time because it authenticates the content of the packages. The authentication system therefore allows manufacturers to avoid use of any expensive security tamper evidencing labeling of packages, additional tamper evidencing structures, etc., while at the same time gaining considerable additional authentication capabilities.

[0036] One implementation embodiment of the authentication system of this invention is described as follows.

[0037] A blister containing 10 tablets has a simple random tablet code sequence of up and down sides, converting to 0's and 1's in a data collection matrix. With 10 tablets, 1024 code sequences are possible. The printed code contains open information, (tablet type, lot number, date and time of manufacturing, manufacturing line, etc.) plus a cryptographic 7-digit hash code, which is generated by cryptographically combining the actual binary tablet code sequence with the open information. As the hash has 7 digits, 10 million hashes are possible, however, out of these only 1024 are possible correct hashes. A reader who knows the cryptographic scheme used (meaning it has the correct keys stored in it) can then immediately decide by simply reading the open information and the hash, if the hash can actually be a true hash or not. In a further step, for true authentication the actual physical binary sequence can be checked. One version or embodiment of these functions is described below with respect to FIGS. 1 through 3.

[0038] An embodiment creating higher level statistical testing is the following. There are n secondary packages (blisters packed in a carton, each carton having a unique product identifier printed on the outside) packed in one larger box, which has also a printed unique

product identifier on its outside. A simple algorithm is assigning a binary number (or any other number for that matter) to each unique product identifier of each carton (for example, if the checksum of the unique product identifier is between 0-4 or between 5-9 gives a 0, resp. 1). Then the packages in the box form a binary (or any other) sequence depending on their position in the box. This sequence can again be encrypted and hashes or similar checks printed on the outside of the box. It is possible to predetermine a given (if possible secret) subsequence and have a shorter code for fast crosschecks. For example, if n=125 in a box, with 5x5x5 cartons a natural subset might be to simply read the topmost 5 codes on the cartons and their corresponding sequence to determine if the content inside the box is likely to be genuine and has not been tampered with.

[0039] Now turning to the flowcharts of authentication operations possible with the authentication system of the present invention, in FIG. 1, the production of an encrypted hash is shown as process 10. The encrypted hash is produced during initial manufacturing/packaging at the beginning of the supply chain (with product manufacturing equipment that uses embossing technology), or during aggregation in the supply chain. The actual product sequence or subsequence 20 (defined by physical attributes and locations of product in a blister pack 24, for example) and open information 22 such as the product, date time, and batch of the blister pack 24 are combined using a hashing algorithm 26 to form a hash value 28. This hash value 28 then goes through step of a private encryption of the hash 30 to form what is printed on the outside of the box 34, including the open information 22 as well as the encrypted hash value 32. From this encrypted hash value 32, the authentication of the package 24 and its contents can be performed in accordance with the invention.

[0040] In FIG. 2, the authentication and verification of the sequence using an encrypted hash is shown in flow chart form as process 110. The top portion of this Figure is the same as FIG. 1, e.g., the actual product sequence or subsequence 20 in the package 24 and open information 22 such as the product, date time, and batch are combined using a hashing algorithm 26 to form a hash value 28. This hash value 28 is compared to a confirmation hash value 120 determined using a public description of the hash 122 applied to the information printed on the outside of the box 34. If the hash values 28, 120 agree at comparison step 140, then the package 24 and its contents are authenticated. The authentication is performed using scanning equipment that only requires a camera and a processor, which may be found in modern smart phones for example.

[0041] In this embodiment, the hash is actively encrypted at hashing algorithm 26 with a private key and decrypted at the public decryption of hash 122 with a public key. This step can be omitted if a secret hashing algorithm is used or a known hashing algorithm is altered in a secret way, for example by using so-called salts and peppers or similar security schemes. Authentication of the product sequence in this particular example then happens by repeating the same hashing procedure and decrypting the printed hash with a public key. If both hashes are identical, the product sequence has not been tampered with, as set forth above. This method does not rely on remote database communication to conduct the necessary authentication.

[0042] In a further embodiment of the invention, the product sequence is encrypted using a symmetric key, the full encrypted sequence or a predetermined part of it is then printed on the outside box, or the back of the blister. For example, FIG. 3 shows a flow chart summarizing this embodiment of authentication using symmetrical encryption, as process 210. The top portion of the diagram shows the production of the package 24, in which the actual product sequence or subsequence 20 is combined with open information 22 such as the product, time, date, and batch, and then the product sequence is encrypted (at step 220) to form what is printed on the outside of the box 34, e.g., the open information 22 and the encrypted sequence 40. The bottom portion of the diagram shows what a user does to authenticate, including reading the encrypted sequence at step 230, using a public/private key scheme to decrypt the product sequence at step 240, resulting in a decrypted sequence 42, and then comparing the decrypted sequence 42 to the actual product sequence 20 at comparison step 250 to determine if the product and package are authentic. When these elements match, the product and package are authentic.

[0043] For authentication, the symmetric key to decrypt the sequences is sent to authorized receivers in encrypted form, using private/public keys to protect the symmetrical key from attacks. This exchange of information is indicated by the double-headed arrow shown extending between steps 220 and 240 in the flow chart of FIG. 3.

[0044] In the virtual world, blockchain-related technologies create blockchains and then distribute identical copies of same on many computers, with the copies being continuously updated and authenticated using various distributed ledger systems depending on the specific blockchain technology being used. In the present invention, the blockchain is physically implemented as the box plus the code on the box, e.g., by using random codes extracted from individual physical product properties.

[0045] While the present invention has been illustrated by the description of various embodiments thereof, and while the embodiments have been described in considerable detail, it is not intended to restrict or in any way limit the scope of the appended claims to such detail. Thus, the various features discussed herein may be used alone or in any combination. Additional advantages and modifications will readily appear to those skilled in the art. The invention in its broader aspects is therefore not limited to the specific details and illustrative examples shown and described. For example, the invention described herein is not limited to application on pharmaceutical blisters, but instead can be used for any product and package which allows to generate a reproducible unique random code for each product for example from a picture taken with a camera. The present invention then takes these individual random product codes and forms a block with them. At each level of packaging these blocks then are formed into a physical blockchain which is cryptographically secured at the next level and so on. Accordingly, departures may be made from such details without departing from the scope of the general inventive concept.

WHAT IS CLAIMED IS:

1. An authentication system for pharmaceutical products, comprising:

product manufacturing equipment that uses embossing technology to form and mark the pharmaceutical products with a coding;

a packaging line that places the pharmaceutical products in one or more packaging defining one or more packaging levels;

in-line reading equipment to determine a product sequence defined by physical attributes and locations of pharmaceutical products in the packaging, the product sequence then being encrypted and used to mark the packaging of the one or more packaging levels with a coding;

scanning equipment at a point in a supply chain downstream from the packaging line, the scanning equipment including a camera that images the codings of the pharmaceutical products and of the one or more packaging levels and a processor that compares the codings to one another to authenticate whether the pharmaceutical products are genuine,

wherein the product manufacturing equipment marks the pharmaceutical products without adding marking products such as inks to the pharmaceutical products, the encryption of the product sequence is achieved using public-private key, and the authentication of whether the pharmaceutical products are genuine is achieved without causing the scanning equipment to communicate with a central data repository away from the supply chain.

2. The authentication system of claim 1, wherein the product sequence is encrypted into the coding for the one or more packaging levels using a hashing algorithm.

3. The authentication system of claim 1, wherein the product sequence is encrypted into the coding for the one or more packaging levels using a symmetrical encryption.

4. The authentication system of claim 1, wherein the scanning equipment further includes at least one of:

a smart phone including the camera and the processor;

a parallel Optical Coherence Technology (pOCT) scanner; and

a time-of-flight camera.

5. The authentication system of claim 1, wherein the system is configured to produce a series of packagings each having a coding, the series of packagings and the codings

collectively defining a blockchain that can be stored and used for authentication at any point in the supply chain.

6. The authentication system of claim 5, wherein aggregation of a group of packagings to be stored in an outer container occurs by forming the blockchain for the group of packagings and cryptographically securing the blockchain for marking on the outer container.

7. The authentication system of claim 5, wherein de-aggregation of a group of packagings stored in an outer container includes only destruction of markings or codings of the outer container but not of the group of packagings.

8. The authentication system of claim 1, wherein the physical attributes defining the product sequence are generated by the product manufacturing equipment, the product sequence being randomized by placement of the pharmaceutical products containing the physical attributes in the locations within the packaging.

9. The authentication system of claim 1, wherein the packaging levels include blister packs into which the pharmaceutical products are loaded, and one or more outer boxes in which the blister packs are loaded.

10. The authentication system of claim 1, wherein the packaging levels include a pill bottle into which the pharmaceutical products are loaded.

11. The authentication system of claim 1, wherein the step of authenticating whether the pharmaceutical products are genuine with the processor automatically provides tamper evidence, thereby avoiding a need for tamper-evidencing structures to be included with the packaging.

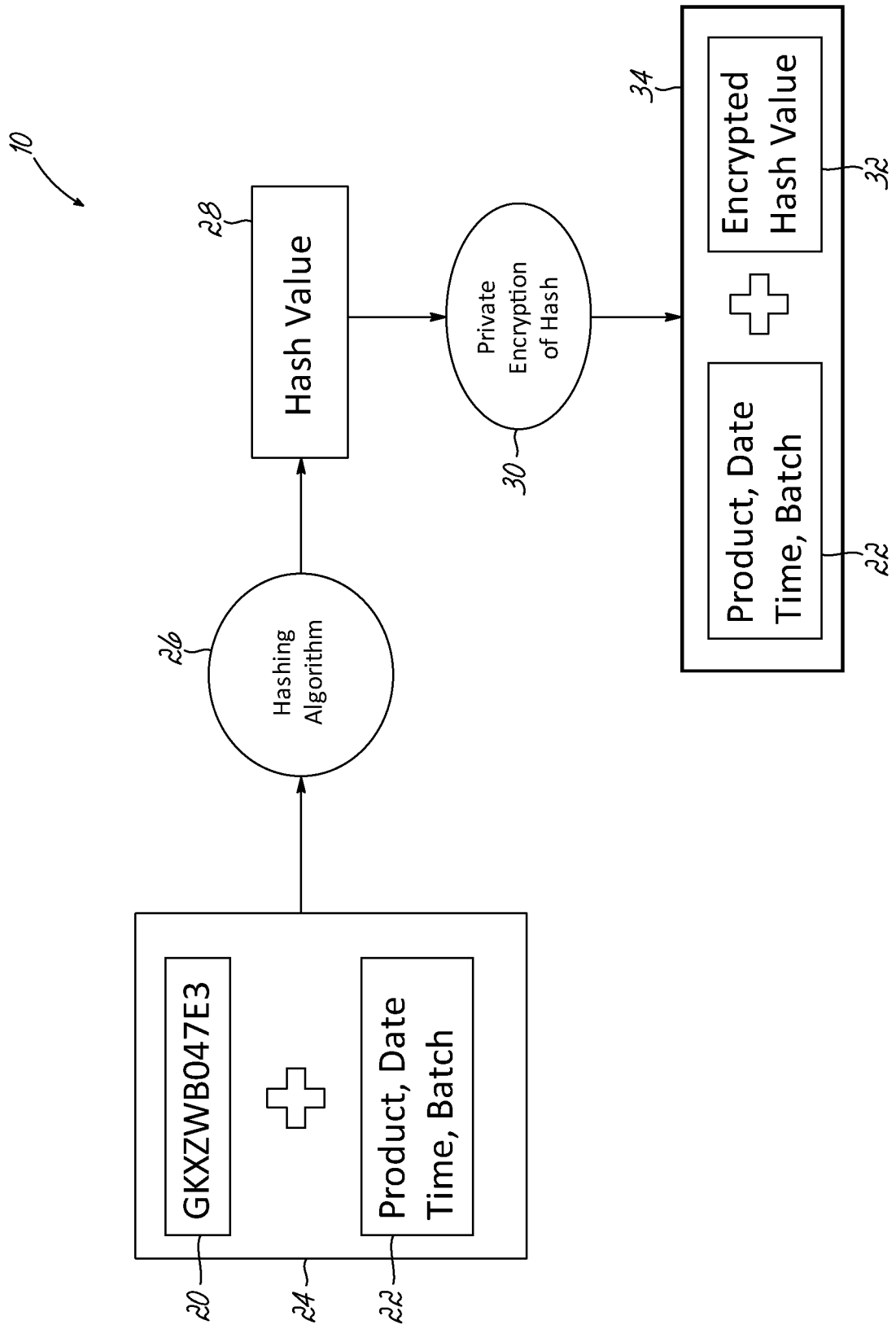

10
GKXZWB047E3
Product, Date Time, Batch
20
24
22
Hashing Algorithm
26
Hash Value
28
Private Encryption of Hash
30
Encrypted Hash Value
32
Product, Date Time, Batch
22
34

FIG. 1

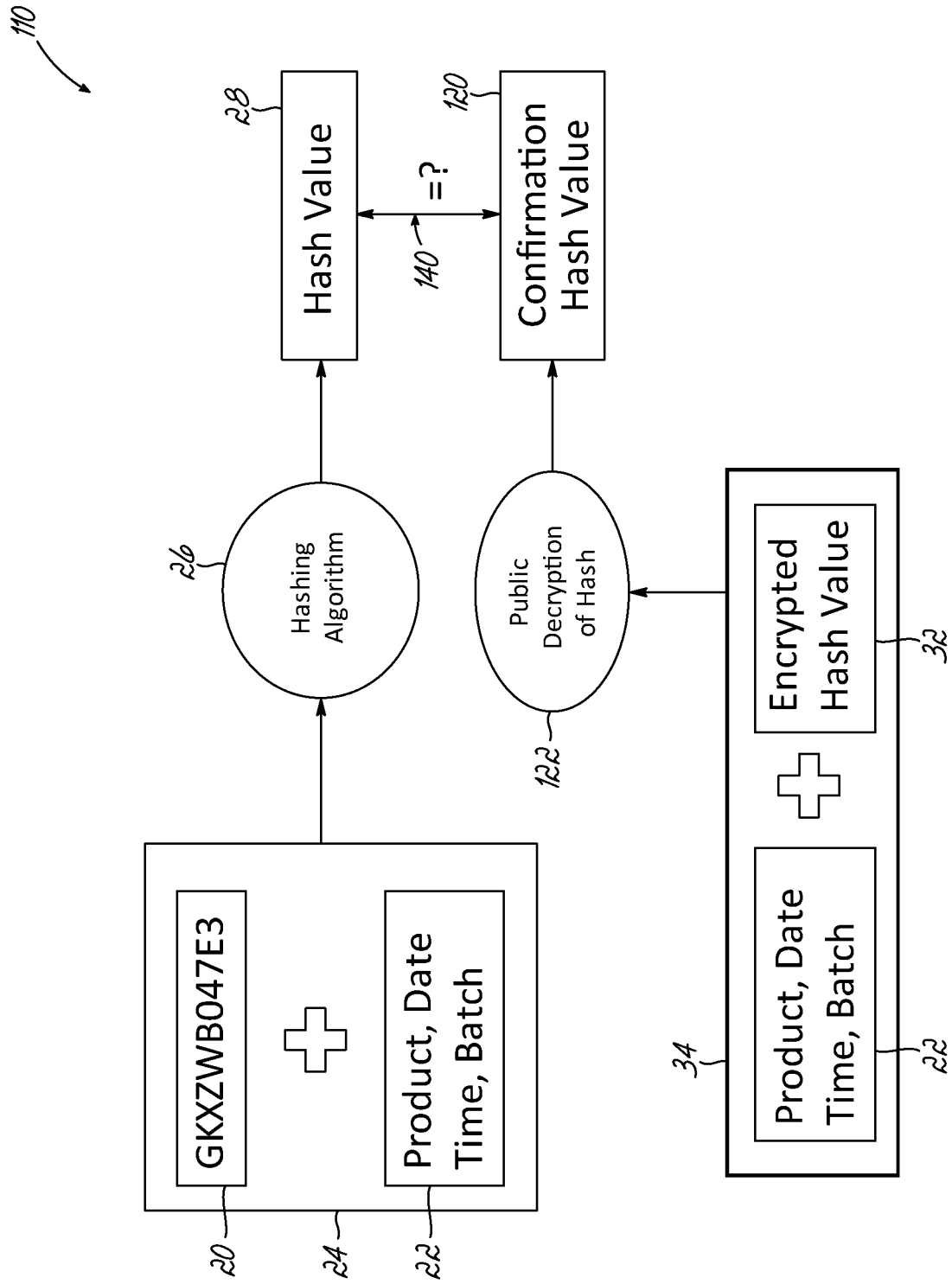

110
28
Hash Value
120
Confirmation Hash Value
=?
140
26
Hashing Algorithm
Public Decryption of Hash
122
Encrypted Hash Value
32
GKXZWB047E3
Product, Date Time, Batch
Product, Date Time, Batch
20
24
22
34
22

FIG. 2

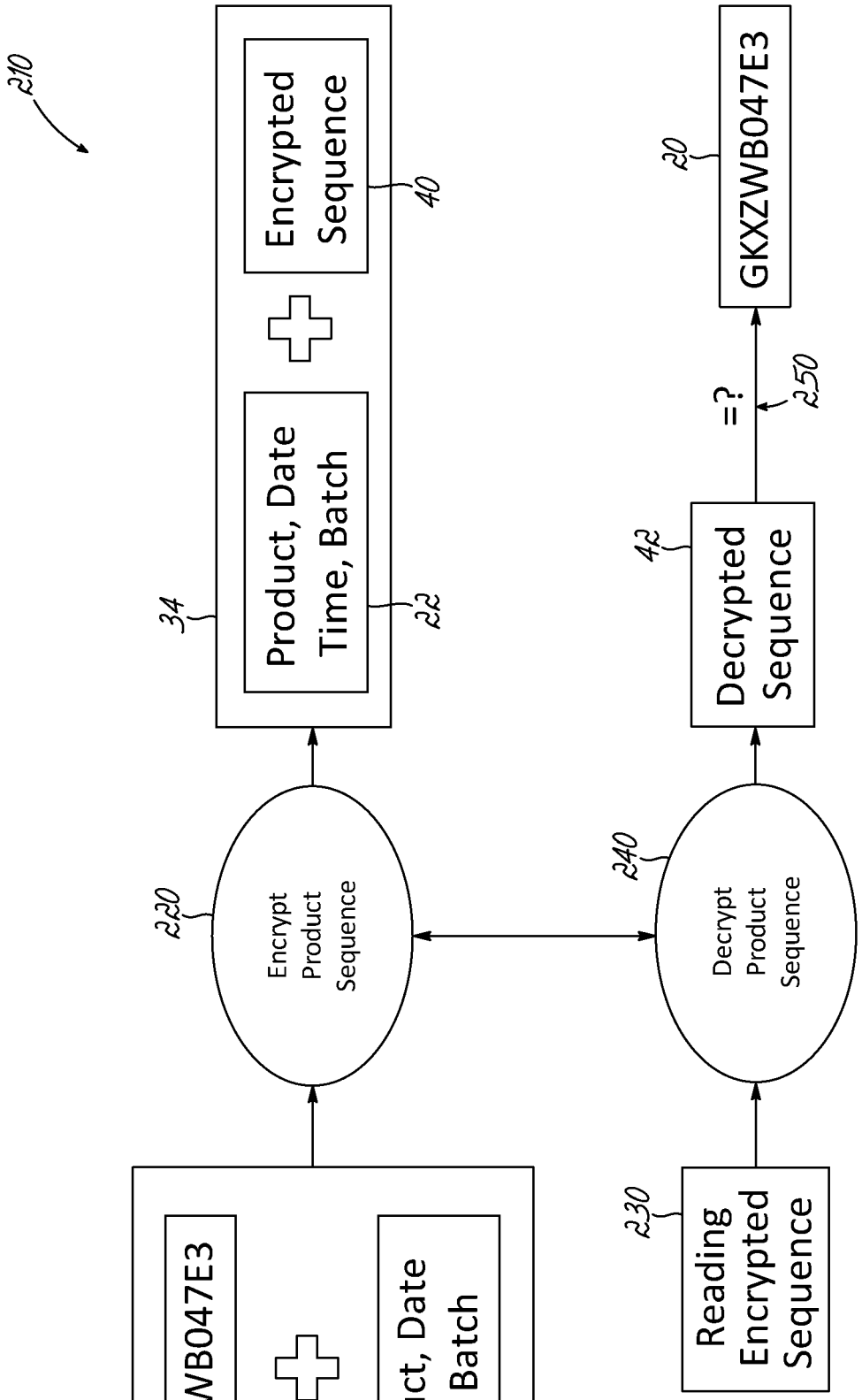

210
GKXZWB047E3
Product, Date Time, Batch
20
24
22
Encrypt Product Sequence
220
Product, Date Time, Batch
Encrypted Sequence
34
22
40
Reading Encrypted Sequence
230
Decrypt Product Sequence
240
Decrypted Sequence
42
=?
250
GKXZWB047E3
20

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US18/30383

A. CLASSIFICATION OF SUBJECT MATTER
IPC - A61J 3/00; H04W 12/06; G06K 9/18 (2018.01)
CPC - A61J 3/007; H04W 12/06; G06K 9/18

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)
See Search History document

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y --- A	WO 2016/172503 A1 (I-PROPERTY HOLDING CORP.) 27 October 2016; paragraphs [0006], [0018], [0021], [0028], [0030], [0039], [0043]; figure 4	1-4, 8, 9, 11 --- 10 --- 5-7
Y	AU 2008/229745 A1 (KIA SILVERBROOK) 30 October 2008; page 25, lines 30-31; figure 21	10
A	WO 2017/027648 A1 (STOLLMAN, J) 16 February 2017; entire document	1-11

☐ 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
"E" earlier application or patent but published on 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
"T" 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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 2018 (12.07.2018)	27 JUL 2018
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774