(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 647 342 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.03.2002 Bulletin 2002/13

(21) Application number: **92911723.2**

(22) Date of filing: **06.05.1992**

(51) Int Cl.[7]: **G07D 7/00**, G07F 7/08

(86) International application number:
PCT/US92/03911

(87) International publication number:
WO 93/22745 (11.11.1993 Gazette 1993/27)

(54) **COUNTERFEIT DETECTION USING RANDOM NUMBER FIELD IDs**

FÄLSCHUNGS - FESTELLUNG UNTER VERWENDUNG VON ZUFALLZAHLEN FÜR DIE IDENTIFIKATIONSNUMMERN

DETECTION DE CONTREFACONS A L'AIDE DE CODES D'IDENTIFICATION CONTENANT DES ZONES DE CHIFFRES ALEATOIRES

(84) Designated Contracting States:
DE FR GB IT NL

(43) Date of publication of application:
12.04.1995 Bulletin 1995/15

(73) Proprietor: **CIAS INC.**
New York, NY 10023 (US)

(72) Inventors:
- **STORCH, Leonard**
  New York, NY 10023 (US)
- **VAN HAAGEN, Ernst**
  New York, NY 10023 (US)

(74) Representative: **Hackett, Sean James**
MARKS & CLERK,
57-60 Lincoln's Inn Fields
London WC2A 3LS (GB)

(56) References cited:
EP-A- 0 010 496
EP-A- 0 177 900
EP-A- 0 315 611
EP-A- 0 354 260
EP-A- 0 372 692
EP-A- 0 426 541
WO-A-86/04170
WO-A-92/05521
FR-A- 2 556 867
FR-A- 2 596 901
US-A- 3 833 795
US-A- 3 890 599
US-A- 4 193 061
US-A- 4 463 250
US-A- 4 558 318
US-A- 4 630 201
US-A- 4 949 256

EP 0 647 342 B1

Description

[0001] The invention disclosed herein relates to counterfeit detection methods.

[0002] When an object, such as a product or document, is worth disproportionately more than the cost of its manufacture, it may be counterfeited at a profit. For example, manufacturers of proprietary products lose billions of dollars each year because their most successful products are often targeted by counterfeiters who produce spurious goods locally or overseas. When counterfeit goods are of similar or identical quality to the original, a manufacturer suffers from a continuous loss of sales as counterfeiting continues unchecked, because detection is difficult or impossible. Inferior counterfeit products may be more easily detected, but in addition to the above, they also jeopardize future sales of non-counterfeited products by marring reputation. In either case, the manufacturer's continuing level of untold lost profits due to counterfeit may be dramatic. Similar concerns arise with counterfeit documents.

[0003] A partial listing of products susceptible to being counterfeited includes: airplane parts; art; auto parts; baby products—formula, diapers, clothing; books; computers; computer peripherals; cosmetics; designer goods—clothing, shoes, eye glasses; electronics; entertainment recordings—CDs, records, audio and video cassettes; games—board, firmware, handheld; military parts; optics—binoculars, cameras; pharmaceuticals; software; tools; toys; watches.

[0004] Documents susceptible to fraud (including counterfeit) include: betting tickets (lottery, sports, etc); bonds (Treasury, commercial, etc); certificates (birth, gift, warranty, etc); checks (personal, commercial, travelers, etc); coupons; credit cards; currency; licenses (driver, business, import/export, etc); passports; scrip (store, amusement park, etc); stamps (postage, food, etc); stocks; tickets (concerts, sports, theater, etc); travel tickets (airline, commuter, etc), and so forth.

[0005] Staggering losses due to counterfeit are estimated. For example, the International Anti-Counterfeiting Coalition, IACC, located in Washington, DC, fears annual losses of $100,000,000,000 (no mistake—one hundred billion dollars!). On April 23, 1990, U.S. Attorney Stephen J. Markman reported the following to the IACC:

"In addition to safety, the economic loss from counterfeit products is enormous: The big three auto-makers estimate that they lose 240,000 jobs each year in the greater Detroit metropolitan area alone due to counterfeiting of auto parts."

[0006] Two approaches for detecting counterfeit are: mechanical—based on conformity, and intellectual—based on uniqueness. These two counterfeit detection philosophies are based on fundamental underlying principles which are diametrically opposed to each other, conformity versus uniqueness.

[0007] Mechanical counterfeit detection techniques require physical examination and/or analysis of the object. The underlying principle here is conformity. Genuine objects are identical to each other while counterfeits must somehow be different. The difference between the genuine and fake must be discernible in order to detect counterfeit. For example, all U.S. currency is printed on special paper. Therefore, if a suspected bill's paper is discovered to be different, the bill is counterfeit.

[0008] Mechanical means alone cannot be relied upon. What one can make or print, another can as well. This creates inherent weaknesses. For example, some counterfeiters of U.S. currency have outwitted the special paper deterrent scheme described above by bleaching the ink off $1 bills and reusing the paper to print $100 bills, while other counterfeiters manufacture their own special paper which is sufficiently similar for their purposes.

[0009] Intellectual counterfeit detection and/or authentication techniques may include signatures, numbers and/or other indicia for coding each genuine object differently. The underlying principle here is uniqueness. Each genuine object is individually signed, or assigned individual identifying information. Traditional ways to individually authenticate objects are: sign or assign.

[0010] One traditional way to authenticate certain objects, namely documents, is to sign them. Each person's signature is effectively different. Even though many may be named John Smith or Chun Lee, i.e., many have the same indistinguishable identifying name, respective signatures are different. Typically, fraud involving documents with individuals' signatures thereon is characterized as forgery, versus counterfeit.

[0011] For example, valid serial numbers may readily be anticipated and printed by counterfeiters using available numbering devices, while forging a signature is another matter. Blank checks, available at stationery stores, for example, may be authorized by John Smith's signature if he is known, or if that signature is verifiable, perhaps by comparison to other signed documents. Signatures, for example, bridge mechanical and intellectual techniques, involving examination-by-eye.

[0012] Applicants' anti-counterfeit techniques address mass produced objects, unsigned products and documents, manufactured to be essentially identical to each other—the only convenient and distinguishable difference among such essentially identical objects being the presence of associated identifying information, such as serial numbers.

[0013] Mr. Smith's signed check, mentioned above, may involve other variable information. For example, the dollar amount, the transaction date, payee information, Mr. Smith's address and bank account number, information about his bank, and so forth. Examples of other articles with variable parameters are: birth certificates, credit cards, lottery tickets, passports, etc.

[0014] Applicants' address how to detect counterfeit objects among essentially identical objects, objects that do not have individually and/or inherently variable parameters, objects such as mass produced products and documents, objects that may be readily identified only by their respective identifying information.

[0015] This is not to suggest that certain aspects of applicants' inventions may not be used beneficially in association with signed documents, for example, to augment the authentication afforded by the signature, for example.

[0016] Another traditional way to uniquely identify objects is to assign serial numbers, by counting, in a most convenient and orderly fashion. However, traditional serial numbers offer little obstacle to a counterfeiter because he can, for example, assign matching ascending and descending numbers given one correct serial number as a start, thereby duplicating authorized numbers only once. Even if two objects with matching serial numbers were found, thereby finding at least one counterfeit, mechanical techniques may still be required to tell which is counterfeit.

[0017] Also, counterfeiters could avoid following a pattern that may be helpful to pursuing authorities if the pattern were discovered. For example, rather than serially numbering their fakes, counterfeiters may randomly select numbering within a wide range of known-to-be valid numbers, so that the possibility of a particular consecutive narrow range of serial numbers being discovered by authorities as having been counterfeited is avoided, making the job most difficult for the authorities (albeit more difficult, but safer, for the counterfeiters as well).

[0018] According to described aspects of applicants' invention, intellectual coding techniques may also offer "self-checking" counterfeit detection schemes (self-checking is a term used with error control coding, adopted for use by applicants when referring to certain intellectual anti-counterfeit coding techniques). Applicants define self-checking as follows: if a single read identifying number does not conform to a secret code, or match up in a database, it must be counterfeit.

[0019] The use of a secret algorithm is disclosed in McNeight et al.'s U.S. Pat. No. 4,463,250. McNeight et al. provides objects with authorized ID numbers that conform to an algorithm or code, so that these ID numbers may be verified or tested for apparent authenticity using the same algorithm. The algorithm is cautiously deployed in locations where it is desirable to detect counterfeit by determining if an object's ID number conforms to the secret algorithm. Caution is required in order to prevent theft or discovery of the algorithm. Authorized ID numbers conform to the algorithm, but the algorithm itself is selected and/or used so that it does not readily allow easy discovery or reverse engineering of the originating algorithm. The algorithm must be kept secret so that it is not also used by unauthorized personnel.

[0020] However, if the secret algorithm were to be stolen or discovered (as a computer "hacker" might delight in doing) one may be worse off with the secret algorithm than without, because a false sense of security could have adverse consequences. Consider for example, what if someone unauthorized discovered the secret algorithm but thereafter kept this discovery a secret from those authorized to use the secret algorithm, so that there was no inkling that the secret had fallen into the wrong hands? Genuine objects authorized by the secret algorithm's ID numbers may then be more vulnerable and susceptible to being counterfeited than if traditional serial numbers had been used in the first place.

[0021] An encryption algorithmic technique used to calculate security codes is disclosed in Peter White's U.S. Pat. No. 4,630,201. White's invention concerns security for checks and other transactions involving money. White uses a table of random numbers. The same table of random numbers is associated both with a portable transaction device and with a bank's central processor.

[0022] For a check, for example, a random number is selected from the table in the transaction device and used to encode the dollar amount of the particular check using an encryption algorithm. The calculated result, a security code, is then put on the check. The authenticity of the security code on such a check may be verified, by recalculating the security code again, in the same manner, in the bank's central processor, and comparing the two security codes for a match.

[0023] We acknowledge the disclosure in US-A-3833795 of a system for designating an object as authorised, by associating it with a serial identification number and a randomly-selected control number.

Summary of the Invention

[0024] The invention disclosed herein utilizes the underlying principle of uniqueness for counterfeit detection. In accordance with the invention, each genuine object is assigned a different authorized identifying code. Counterfeit is detected when incorrect, repeated or out-of-place ID numbers are found on objects. ID numbers which are associated with objects may be represented in normal alphanumeric characters or otherwise, such as OCR or MICR fonts of alphanumeric characters, decimal characters, or bar coded characters, etc., which are designed to be machine read, and may be visible or substantially transparent.

[0025] In particular, an object's identifying serial number may be appended with one or more distinct random portions, positioned to the right of the serial portion, for example, with or without a decimal point (or binary point if binary were being used) or positioned preceding the serial number, or the serial portion may be understood as including one or more random portions, etc.

[0026] A truncated security ID number, comprised of a distinct serial number portion and a first random portion, may be used, for example, on the outside of a product package, and a complete security ID number, with a second random portion along with the serial number and said first random portion, used inside a product's packaging (concealing the complete ID number from casual perusal) such as on a product's enclosed return warranty registration card. Each distinct random portion may include one or more randomly selected digits.

[0027] Objects of the invention disclosed herein are to protect proprietary product and document integrity, quality, reliability, safety, authenticity and the like, by creating hurdles for would-be counterfeiters, and thereby reducing or eliminating such illegal, dangerous and/or economically devastating activity.

[0028] In so far as counterfeiting may nonetheless persist, it is another object of this invention to reduce investigative and/or prosecution effort, by providing those pursuing and/or prosecuting counterfeiters with irrefutable evidence, such as products or documents with unauthorized ID numbers, and therefore undeniably counterfeit, so that such culprits can be stopped from foisting their bogus, and typically shoddy, goods on society, and from unfairly competing with more honest commerce.

[0029] Other objects of the invention are to improve counterfeit detection and/or deterrence, to apprehend and/or track criminals and/or deter crime.

[0030] In accomplishing the above and other objects, individually and in various combinations, the applicants devised coding in accordance with their inventions, particularly but not exclusively for bar codes.

[0031] In accomplishing certain of the above objects of the invention, applicants have expanded upon and improved the counterfeit detection techniques disclosed in their U.S. Patent No. 4,814,589 and copending patent applications mentioned above. According to their invention, such techniques involve accountability, alone or in combination with techniques which make it difficult to copy visually detectable features, such as holograms. The invention may be applicable to almost all types of counterfeitable objects.

[0032] The present invention provides methods and systems for identifying unauthorised objects, as defined separately in dependent claims 1 to 6, 9 and 11.

[0033] The invention and its background are described with particular reference to ID numbers, and bar coded ID numbers, in decimal, base ten, but which may be represented in any base such as binary, ternary, octal, decimal, base 43, etc. However, the invention has wider application and it is not intended to limit the scope of the invention by such references.

Description of the Drawings

[0034] The invention is illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references, if any, indicate like parts, and in which:

FIG. 1 is a plan view of a product return card with ID number indicia in decimal digits and in bar code. The product return card may be found inside a product package. The ID number indicia include two random portions, shown as 23 and 17.

FIG. 2 is a side view of the outside of a product package with ID number indicia thereon corresponding in part to the ID number indicia on the product return card of Fig. 1.

FIG. 3 is a side view of the outside of a product package with ID number indicia thereon corresponding in part to the ID number indicia on the product return card of Fig. 1. Also located on this same outside side near said ID number indicia is a standard UPC bar code symbol.

Detailed Description

[0035] Many products already include registration material, such as a blank *name, address, where purchased* form, printed on a return postcard on which may be found the product's ID number. Such cards are often used to activate a product's warranty.

[0036] Counterfeit products may be detected by looking for duplicate registration of normal serial numbers. However, this procedure leaves something to be desired, because counterfeit cannot be detected via the serial number until two (or more) of the same serial numbers are eventually registered, and even so, when two of the same serial numbers do turn up, an investigation must first be made to determine if one is genuine (as both may be fake) and if so, which one. Also, assuming a counterfeit product is positively detected and the vendor who sold the counterfeit product is identified by the product registrant, it may still be impossible, or cumbersome at best, to determine if other products in the vendor's stock are also counterfeit. Further, physical examination procedures would likely be "intrusive" and may render examined products unfit for retail sale.

[0037] In a way, these difficulties arise from the use of traditional serial numbers. Because traditional serial numbers are as orderly and convenient to use as possible, they are also completely and readily predictable, and thus are directly vulnerable and susceptible to being counterfeited.

[0038] Applicants' telling anti-counterfeit technique overcomes these shortcomings: registration involving just one ID number on a counterfeit product can immediately and unmistakably be identified as fake, and even before a "lead" from the registration process, counterfeit products can be positively identified on the retail shelf or in mail order inventory warehouses or distribution channels, etc., without opening the product's packaging.

[0039] According to the invention, ID numbers include a serial portion and one or more random portions appended to, or associated with, the serial portion. Such ID numbers have the serial portion in predefined digit positions, so that ID numbers may be used just as orderly and conveniently as traditional serial numbers. The serial number portion (which may be called the serial field) of the ID number is appended with one or more random portions (each random portion may be called a random field). Each random portion may contain one or more randomly selected digits. A random number generator may be used which may, e.g., randomly select digits based on cosmic noise. Required randomly selected numbers may be provided on-the-fly, as needed, and then stored if required or erased if not required. Or, required randomly selected numbers may be generated and stored in a list and the list then referred to as required. It may be useful for random portions to be separated from the serial portion by a decimal point, for example.

[0040] Security is enhanced because such complete authorized ID numbers are unpredictable as follows: if one decimal digit is randomly selected, only one in ten ID numbers would be predictable by a counterfeiter, and if two digits are randomly selected, only one in a hundred, etc. There is no secret code to be stolen or discovered. With applicants' random technique, the problems and worries described above for traditional serial numbers and ID numbering in accord with a secret algorithm are simply avoided.

[0041] For example, the serial random number (SRN) shown on the Product Return Card in Fig. 1 is:

123456 23 17

For example, this ID number, 123456 23 17, is associated with a genuine product. The first six digits of the ID number, 123456, comprise a traditional sequential serial number with sufficient range to uniquely identify one million genuine products, from 000000 to 999999. The next four digits, in this example 23 and 17 (shown throughout herein with separating spaces for clarity) are randomly selected, and stored in a file, such as a computer file, perhaps a file associated with a database system, along with the traditional serial number portion, to form a file listing of complete authorized ID numbers. In other words, aside from associating authorized ID numbers with authentic objects, authorized ID numbers are also stored separately, e.g., on a list stored in a computer file. Because of the serial portion, the list of complete authorized ID numbers is as orderly as can be, and because of the randomly selected parts, it is also unpredictable as described.

[0042] For example, when a product's ID number, e.g., 123456 23 17, is entered from the return card in a product registration system computer containing the listing of complete authorized ID numbers, the random digits can be checked automatically—if they do not all match those which were originally stored, a counterfeit product's unauthorized ID number is positively and immediately detected. The product registration system computer may also be used by investigators looking for counterfeit, without need for registration and/or return cards, as described below.

[0043] In this aspect, complete authorized ID numbers simply cannot be effectively predicted or anticipated without one-for-one copying from complete genuine ID numbers by the counterfeiter, which is prohibitive, or, at least severely limiting, creating a hurdle for the counterfeiter.

[0044] Corresponding ID numbers, or preferably ID numbers corresponding only in part, may also be put on the outside of product packaging. The truncated serial random number (SRN), which corresponds in part to the ID number indicia shown in Fig. 1, is shown in Fig. 2 on the Product Package as:

123456 23

The reason for truncation is described below. Use of such ID numbers on the outside of product packaging makes them readily accessible, and allows a "shopping" service contracted by the product's manufacturer, or an investigator, to read and store bar coded ID numbers from products, e.g., on store shelves, and then send them, for example using a modem, to the manufacturer's system registration computer where the randomly selected portion of the ID numbers read from products can be checked against the stored list of complete authorized ID numbers, so that unauthorized ID numbers from counterfeit products may be detected. Thus, counterfeit products may be identified even before customer purchase, and authorities may be put on the trail of the perpetrators sooner. In enforcement proceedings, even good leads can get cold.

[0045] Or for example, applicants' counterfeit product detection system could be set up to include handheld devices that combine radio communication capability with bar code reading (e.g., the LRT 3800, which also includes portable computer terminal capabilities, in a handheld unit, a product of Symbol Technologies Inc., of Bohemia, New York) so that counterfeit could be detected at about the speed of light while an investigator points the device at a product being checked for authenticity. For example, the LRT 3800 device reads and interprets the ID number bar code on a product that may be counterfeit, radio communicates this information to the product registration system computer to automat-

ically check the ID number's random digit(s) to see if they match what was originally stored, and then receives back from the computer an indication if the ID number is unauthorized, thereby detecting counterfeit.

[0046] The type of equipment used by Federal Express delivery service may be adapted for applicants' counterfeit detection system. Federal Express uses bar code reading and communication devices, and sometimes a communication satellite, in a package tracking system (see *Automatic ID News* Vol. 7, #2, 2/91, pg. 16). With such devices working with a central anti-counterfeit computer system, for example, counterfeit could be detected quickly, on a shelf in a location being checked for having counterfeit product, at a U.S. border in a routine or special Customs inspection, and so forth.

[0047] If a counterfeit product with an unauthorized ID number did turn up in the registration process, a shopping service or an investigator could be dispatched directly to the location that sold the counterfeit and/or to this seller's supplier, to check for additional counterfeit products, without opening product packaging. Such investigation may be conducted covertly if there is suspicion that the vendor himself may be implicated. (Bar code readers with storage, for example, only the size of a credit card, are commonly available.)

[0048] With bar coded ID numbers on the outside of packages, investigative effort is reduced, and subsequent prosecution effort may be simplified, because prosecuting attorneys may have irrefutable evidence: e.g., product with an unauthorized ID number, and therefore counterfeit.

Dual Random

[0049] ID numbers located on the outside of packaging are more accessible than ID numbers located inside the packaging, and may therefore more readily allow the possibility of a counterfeiter acquiring authorized ID numbers from the outside of genuine product packaging than from the inside (this may not be a significant risk in all cases). For example, a counterfeiter might bribe someone in a distributor's shipping/receiving department to accumulate "outside" authorized ID numbers with a concealable bar code reader so that they could be used later on counterfeit products. If this happened, the manufacturer could be back where he started, looking for duplicates, suffering the shortcomings mentioned above, or perhaps even being worse off because of a false sense of security.

[0050] Applicants' anti-counterfeit invention anticipates this possibility. For example, the complete authorized ID number, 123456 23 17, is printed on the return registration card (as shown in Fig. 1) which is located inside the package and is therefore less accessible than the ID number located on the outside of packaging, thus concealing the complete authorized ID number from casual perusal. For example, if a product is in its original packaged condition, an ID number with associated random portions located inside the packaging would be concealed.

[0051] Only a truncated authorized ID number, 123456 23, is printed on the outside of the package (as shown in Fig. 2). Thus, even if a counterfeiter surreptitiously acquired outside ID numbers from product packaging, counterfeit products can still be detected immediately upon registration, and also with absolute certainty, and still without relying on the appearance of duplicate registration ID numbers.

[0052] If the first two random digits of inside ID numbers are correct, and only the last two random digits are wrong, the manufacturer need not go looking for incorrect outside ID numbers on any shelves, so to speak, because it is evident that the counterfeiter somehow acquired authorized (but truncated) outside ID numbers.

[0053] In this case the manufacturer is still not without help from the system computer, by which this discovered "leak" may be dealt with, and this now notorious counterfeiting ring broken. Indeed, it may well be possible to catch culprits "in the middle," by analyzing when the products with the copied outside ID numbers were manufactured and through what distribution channels they moved, as well as backtracking the source of the counterfeit product itself.

[0054] In an embodiment of applicants' invention, a list (e.g., a partial listing limited to specific ranges of serial numbers, and/or selected geographical and/or chronological parameters, etc.) of authorized outside ID numbers (in the above example, 123456 23) might be supplied in a portable, non-communicating unit to investigators for use in the field as described below. For increased security, perhaps specially trusted investigators only would be supplied with such "portable" lists, and/or such lists may only be supplied just prior to an investigation at a given location, and/or such lists may only be supplied in units that automatically erase the list after a given amount of time has elapsed and/or at a specified time, etc.

[0055] In any case, this embodiment is less of a security exposure than supplying complete ID numbers for use in the field, especially if only a limited, partial listing is provided. For example, even if a portable list was acquired and used by counterfeiters, more complete ID numbers, such as those from a return card, would still expose the crime.

[0056] For example, with portable lists counterfeit objects may be detected immediately, in the field, by comparing ID numbers read from a product's packaging directly against the list to determine if the correct random field for a respective serial number field is present on a product's package, without checking with the central computer where the master list of complete ID numbers is stored, on-site so to speak, no communications required, using a portable unit (much as checking a hot list, described below). Thus, increased convenience, effectiveness and cost saving (e.g., limited communication requirements) may be realized when looking for counterfeit, without undue security exposure.

Security Enhancements

[0057] Additional security enhancements are possible. For example, to prevent unauthorized copying of ID numbers, a return card's complete ID number, or just the random security part(s), may also be concealed, e.g., with latex covering, like the VIRN number (Void If Removed Number) on an instant lottery garre ticket, or the ID number may only be represented on the card in a customized "secret" bar code format.

[0058] Variations are possible. For example, if the possibility of a counterfeiter acquiring outside ID numbers during distribution exists, and return cards are not appropriate for a given product line, several such products may be packed for shipping in a sealed carton concealing the products' outside ID numbers during distribution.

[0059] Also, outside ID numbers can be put on such cartons, and latex-covered *return from the retail vendor* cards can be put in the carton (but not inside individual product packaging).

[0060] And, as described below, the use of, e.g., 123456 17 instead of 123456 23 17 on a return card, adds security.

Four Random Fields

[0061] In another example, consider an ID number with four appended random fields:

123456_ 23 17 79 10

The blank ligit position shown with an underline is described below. 123456 23 may be put on the outside of a shipping carton containing ten products. 123456 23 17 may be latex-covered and put on a *return from the retail vendor* card and located inside the carton, but not inside individual product packaging.

[0062] Ten ID numbers using 123456_ 23 17 79 may be used as follows, one on the outside of each product package:

1234560 23 17 79
1234561 23 17 79
1234562 23 17 79
1234563 23 17 79
1234564 23 17 79
1234565 23 17 79
1234566 23 17 79
1234567 23 17 79
1234568 23 17 79
1234569 23 17 79

Each may be applied to ten respective product package's outside. The additional digit in each of these ID numbers (in the seventh position from the left, shown underlined) uniquely identifies each of the ten products, for the batch serial number 123456, and may conveniently be considered as part of the serial number portion of the ID number for individual products.

[0063] Each product may also have a return card inside its packaging, each with one of the following ID numbers:

1234560 23 17 79 10
1234561 23 17 79 10
1234562 23 17 79 10
1234563 23 17 79 10
1234564 23 17 79 10
1234565 23 17 79 10
1234566 23 17 79 10
1234567 23 17 79 10
1234568 23 17 79 10
1234569 23 17 79 10

[0064] If this type of embodiment were used, one risk is that a savvy counterfeiter obtaining one correct ID number from a return card, such as 1234567 23 17 79 10 in this example, might correctly deduce nine other authorized ID numbers, those others between: 1234560 23 17 79 10 and 1234569 23 17 79 10, inclusive.

[0065] Because of the difference in the number of digits in ID numbers for respective locations, when ID numbers are read it may readily be automatically determined by apparatus where that ID number was read from, whether from the outside of the carton of ten products, from inside the carton on the carton's return card, from on the outside of an individual product or from the return card inside the individual product package.

[0066] In the event of counterfeiting of authorized ID numbers such as these, knowledge of which random digits have

been copied provides useful information, e.g., when and/or from where the ID numbers were copied. For example, if:

1234560 23 17 79 86

(and other similarly constructed ID numbers) were found on a counterfeit product, a counterfeiter learned correct ID numbers for three places: the outside of the carton, inside the carton, on the outside of an individual product, but not for the product's return card. This would indicate that the counterfeiter had access to the outside of the products' individual packaging for copying, since all random digits up to that point are correct.

[0067] However, in some embodiments it may be preferred to increase security. For example, additional security may be realized if the random fields are used more sparingly. For example, while 123456 23 may be used on the outside of the carton of ten products, only 123456 17 may be used on the carton's return card (instead of 123456 23 17). 1234560 79 (the first of ten similar ID numbers corresponding to the above) may be used on the outside of an individual product, and 1234560 10 (again, the first of ten) used on the return card inside an individual product package. Now, for example, knowledge of a valid ID number from the outside of an individual product, 1234560 79 in this example, does not inform of the corresponding random field for the outside of the carton of ten such products (23), or of the corresponding random field used inside the carton on the carton's return card (17). Thus, higher security is realized.

[0068] However, in this example of higher security, inquiries made in the system computer to check an ID number for authenticity, i.e., whether or not the random field digits are correct, would need to inform from where the ID numbers were read. For example, while 123456 23 is correct for the outside of a carton of ten products, 123456 17 is incorrect. 123456 17 read from the wrong location (the outside of a carton) would be an unauthorized ID number and indicate counterfeit.

[0069] In another embodiment, say the following ID number (with a sixteen digit serial field and five fields of two randomly selected digits each):

1234567812345678 23 17 79 10 55

were used for documents, for example, on U.S. currency. A file with the serial number portions and only the associated first random field, shown with 23 in this example, may be provided by the Bureau of Engraving and Printing to commercial banks for their general use in detecting counterfeit, a file of the random fields 23 17 provided to Federal Reserve Banks for their use, a file of the random fields 23 17 79 to the Treasury, FBI, CIA, etc., a file of the random fields 23 17 79 10 may be used exclusively by those most trusted in the Secret Service, and a file of all five random fields, 23 17 79 10 55 may be stored for safe keeping and used with extreme caution only if ever needed. In this manner, if sophisticated counterfeiting were to occur, authorities would know exactly where to start looking for culprits.

[0070] Bear in mind however, that currency with complete ID numbers would be in circulation, and complete correct ID numbers may therefore be copied one-for-one therefrom in large quantities over extended periods. But, if such sophisticated counterfeiting and preparation therefor was carefully committed over an extended period, archived currency flow information, as and if available, may reveal to authorities patterns of when and where authentic currency ID numbers copied from were situated in order for this copying to occur, thereby providing a possible lead for pursuers to follow.

Random and/or Secret Code

[0071] It may be useful in some counterfeit detection applications to provide ID numbers verifiable in some fashion in accord with a secret algorithm. For example, this may be accomplished according to applicants' invention as described above, i.e., to append to a serial number one or more distinct portions that conform to one or more respective secret codes. Such portions may be called secret code fields. In addition, random fields may or may not also be appended to the ID number.

[0072] In the first example, one secret code field is appended to the serial number (random fields are not used in this first example). The secret code field is represented by the ?? (the appended secret code field being undetermined thus far). The first example:

First example: 123456 ??

[0073] The second example uses two appended random fields (each random field has two randomly selected digits in these examples) and one appended secret code field (containing two digits that result from calculating a code in these exarr ples) all three of which (fields) are used in a manner independent of each other. The secret code field is represented by the ?? (the appended secret code field being undetermined thus far). These three fields are shown in the second example as follows:

Second example: 123456 23 17 ??

[0074] The following technique may be employed to calculate the secret code field for both the first and second

example. To the sum of the digits of the serial number portion add one, multiply by 541 and then divide by 11:

$$1 + 2 + 3 + 4 + 5 + 6 = 21 + 1 = 22 \times 541 = 11{,}902 \div 11 = 1082.0000$$

Do not use the result—only use two digits, the two digits located on either side of the decimal point (2.0) in reverse order (02) in the secret code field, as shown for the first and second example:

First example: 123456 02
Second example: 123456 23 17 02

[0075] In this independent manner, knowledge of any random field (used in the second example only) is not required to use the algorithm on a serial number in order to calculate the secret code field to be appended thereto.

[0076] Say the secret code's algorithm required that the sum of the two digits of the first random field (shown as 2 and 3 in this second and third example) need also be added to the sum of the digits of the serial number portion, the complete secret code working for the third example as shown:

Third example: 123456 23 17 ??

[0077] In this technique as described, according to this aspect of the invention, the serial number and the random number may be employed to calculate the secret code field for the third example as follows:

$$1 + 2 + 3 + 4 + 5 + 6 + 2 + 3 = 26 + 1 = 27 \times 541 = 14{,}607 \div 11 = 1327.9091$$

7.9 reversed, 97 would be the final result for the secret code field in the third example as shown:

Third example: 123456 23 17 97

[0078] In this third example, in a dependent manner, knowledge of both digits of the first random field is required to calculate the secret code field.

[0079] In this third example therefore, knowledge of the authorized random numbers of the first random field for respective serial numbers would be needed by those who may be anticipating verifying the secret code field of an ID number. While dissemination may tend to put the "sensitive" random information at (increased) risk of exposure, the use of random as described may also tend to increase the difficulty of breaking the secret code if the random information did not fall into the wrong hands (bear in mind any possible one-for-one copying as well).

[0080] The random digits used for calculating the secret algorithm need not be disseminated at all. The random digits used for calculating need not be put on the authorized objects themselves. Only some result of the secret algorithm calculation may be put on the authorized object and, according to the invention, the random digits required for the algorithm calculation stored only in the central computer, i.e., the random digits are stored in one location only. The advantage of this is reduced exposure of the random numbers, and increasing security for the secret code.

[0081] The fourth example following uses the same secret code algorithm as the third example, but the random field represented by 17 in the third example is not used at all, and the random field represented by the 23 in the third example is used in calculating the algorithm in the central computer but it (23) is not put on the authorized object. Thus, in this fourth example, serial numbers have only one respective random field which is only stored in the central computer and is not put on the object. The fourth example:

Fourth example: 123456 ??

[0082] The complete secret code employed in the central computer to calculate the secret code field for the fourth example is shown working as follows, the random digits, 23, being stored only in the central computer and retrieved for use when calculating the algorithm for serial number 123456:

$$1 + 2 + 3 + 4 + 5 + 6 + 2 + 3 = 26 + 1 = 27 \times 541 = 14{,}607 \div 11 = 1327.9091$$

7.9 reversed, 97 would be the final result for the secret code field in the fourth example as shown:

Fourth example: 123456 97

[0083] In a first embodiment of this fourth example, the algorithm may be calculated for authorization and the result put on the object being authorized, and calculated again for verification. In order to calculate again for verification, the random numbers need to be kept in storage to be used again in the calculation. In this case, the secret code field result of the calculation is put on the authorized object but need not be stored aside from the object. Therefore, in order to lessen exposure of sensitive information, means may be provided for automatically erasing the calculated secret code field results after being put on the authorized objects.

[0084] Or, in a second embodiment of this fourth example, when the algorithm is calculated for authorization and the result put on the object being authorized, the result could also be stored in the central computer, in association with the serial number, until needed again for verification of the authenticity of the object. In this second embodiment, verification then would work as follows: the serial number including the secret code field would be read from an object having its authenticity checked, and the reading compared in the central computer against the result that was previously calculated and stored for this serial number. A match indicates genuine.

[0085] Since the random numbers are not needed again for calculating in this second embodiment of the fourth example, the random numbers need not be kept in storage after the authorization process. If the secret code field result of the calculation is stored, random numbers need not be. The random numbers may be erased after the calculation. Advantage: risk of exposure of the random numbers is then eliminated and this would tend to increase the difficulty in breaking the code, as mentioned above. Also, if the random numbers required for this second embodiment of the fourth example were only provided on-the-fly, as needed for the calculation, and erased immediately after the required calculation is completed, security would be increased. For example, means may be provided to automatically erase the random numbers after the calculation.

[0086] Notwithstanding the above, even sensitive data may need to be securely protected for backup or archival purposes in a given computer application, to protect against loss of valuable information from possible hardware failures, such as a head crash on a hard drive, damaging dirt, power failure, operator error, theft, accident, war, acts of nature such as lightening, earthquake, etc. However, secured storage for backup or archival precautions should not be confused with dissemination of stored sensitive information (such as random information, secret code fields and secret algorithms) needed, for example, to verify ID numbers at more than one location. Such dissemination for expected use such as verification may tend to put sensitive information at increased risk of exposure, thereby increasing the possibility of sensitive information becoming available to counterfeiters.

[0087] According to applicants' invention, security is increased because authorization and verification is performed in only one location, and the random numbers and/or the secret code and/or the secret code fields need not be disseminated beyond this central system nor stored longer than needed (except that ID numbers, however they are constructed, are associated with the authentic objects they protect) and therefore the risk of exposure of the random information and/or the secret algorithm and/or the secret code fields is lessened.

[0088] In the fifth example following, everything works just like the fourth example but with one exception—a random field, shown as 17 in this example, is used independently as follows:

Fifth example: 123456 17 ??

[0089] In the fifth example, the secret field is calculated, and verification may be accomplished, just as described for the fourth example, storing the required random digits safely in one location (according to the first embodiment) or storing the secret code field in one location (according to the second embodiment).

[0090] In the fifth example, the random digits, 17, are put on the object and stored in the central computer as described previously. The fifth example's ID number is completed as follows:

Fifth example: 123456 17 97

[0091] In summary:

First example	123456 ?? to 123456 02
Second example	123456 23 17 ?? to 123456 23 17 02
Third example	123456 23 17 ?? to 123456 23 17 97
Fourth example	123456 ?? to 123456 97
Fifth example	123456 17 ?? to 123456 17 97

[0092] In the first example, 123456 ??, the secret code is independent and random is not used at all. In the second

example, 123456 23 17 ??, the secret code is used independently, and two random fields are used. In the third example, 123456 23 17 ??, the secret code is dependent on one random field (which is also put on the object) and one random field is independent of the secret code. In the fourth example, 123456 ??, the secret code is dependent on one random field but this random field is not put on the object; this random, or the secret code field, is stored in only one computer. In the fifth example, 123456 17 ??, the secret code is dependent on one random field but this random is not put on the object; the random, or the secret code field, is stored in only one computer, and one random field is independent of the secret code.

[0093] If a secret code is to be used with or without random in ways described above, special consideration need be given to the worry that the secret code might be broken. Perhaps the lesser exposure in this regard is when a secret code is used with random in a dependent manner as described for the fourth and fifth examples. The secret code might be particularly vulnerable in the first and second examples.

[0094] In some applications, the use of a secret code may add significant difficulty for counterfeiters, i.e., in addition to other requirements, a counterfeiter would require knowledge of the secret code and he would be required to operate this code in order to provide correct ID numbers for his fakes. Some counterfeiting may therefore be deterred.

[0095] In another example following, certain variations are described. One digit that cannot be anticipated is calculated using part of an object's six digit serial number and a random number. The random number is used in the calculation but it is not associated with the object in this example:

123456 ?

The serial number portion is 123456. The digit that cannot be anticipated is represented by the ? as this digit is so far unknown but it will be calculated below.

[0096] The following algorithm may be employed to calculate the digit that cannot be anticipated for this example. Referring to the serial number portion, 123456, from left to right, add the fourth digit (4) to the product of the fifth digit (5) times three, and to this sum add the product of the sixth digit (6) times seven. Divide this sum by a randomly selected number. For this example a one digit number is randomly selected: 9. The calculation as described is shown as follows:

$$4 + (5 \times 3) = 19 + (6 \times 7) = 61 \div 9 = 6.7777$$

Calculate to four places and do not round the fourth place to the right of the decimal point (as shown). Now add the digit to the left of the decimal point, 6, to the third digit to the right of the decimal point, 7, but round this third digit up before adding if the adjacent fourth digit is between five and nine inclusive. In this example then, the third digit to the right of the decimal point, 7, is rounded up to 8. Therefore, 6 + 8 = 14. Now calculate the arithmetical complement of the digit located to the left of the decimal point, 4, as follows: 10 - 4 = 6. Use this result for this example as shown:

123456 6

[0097] Thus, the serial number 123456 and the respective digit 6 may be used to designate one object among as many as 999,999 other essentially identical and identifiable objects in this example as authorized. For example, each such object may be identified by a respective ID number which includes a six digit serial number portion. And, because a random number is used in the calculation with part of the serial number, the resulting digit (6 in this example) cannot be anticipated.

[0098] In this example, the randomly selected digit for serial number 123456, 9, which is used in the calculation, may be stored and retrieved and used to recalculate the digit that cannot be anticipated (6) for verification. Or, the digit that cannot be anticipated, 6, can be stored (aside from being associated with the object) and retrieved for verification purposes without recalculating the algorithm.

[0099] Also, referring to the outside Product Package ID number shown in Fig. 2, 123456 23, a secret algorithm may also be used to provide a corresponding inside ID number, shown as, 123456 ??, which may be used, e.g., on a return card. For example, the serial number, 123456, and the random number, 23, may be used to calculate the secret code field for a corresponding inside ID number as shown for this example:

$$1 + 2 + 3 + 4 + 5 + 6 + 2 + 3 = 26 + 1 = 27 \times 541 = 14{,}607 \div 11 = 1327.9091$$

As above, 7.9 reversed, 97 would be the final result for the secret code field for the corresponding inside ID number shown for this example: 123456 97.

[0100] In applicants' techniques described above, multiple secret code fields, each using a different secret code convention, in various combinations with one or more random fields, may also be used to provide different levels of counterfeit resistant ID numbers.

Repeated ID Numbers

[0101] Applicants' preferred anti-counterfeit system also checks for repeated ID numbers (inside, outside, etc). This prevents the possibility of one or a few authorized ID numbers used over and over going undetected. Repeated authorized ID numbers may be found, as well as repeated incorrect ID numbers. For example, two or more similar objects may be located with the same correct (or the same incorrect) ID numbers.

[0102] Repeated ID numbers could be flagged in the system computer and put out on "hot" lists and automatically circulated to authorized investigators to allow "immediate" detection of each subsequent use, as described below. Or, for possible security reasons, it may be preferred to maintain hot lists only in the system computer. For example, a hot list of repeated valid ID numbers in New York may be useful to a counterfeiter in California, if, for example, California investigators did not have the hot list of repeated valid numbers that had been circulated to investigators in New York.

[0103] Notwithstanding, there is an advantage to authorities looking for repeated ID numbers (valid or invalid) when compared to looking for wrong ID numbers: circulating a hot list (of repeated numbers) to investigators in the field (perhaps loading the hot list into Symbol Technologies' LRT 3800 unit mentioned above) is certainly less of a security exposure than circulating the master list of stored complete ID numbers in the field. The hot list of repeated numbers may be used relatively safely by investigators in the field when helpful for pursuing counterfeiters. For example, counterfeit objects may be detected in the field, without checking with the central computer where the master list of ID numbers is stored, on-site so to speak, no communications required, using a portable handheld unit.

[0104] The more often authorized ID numbers are repeated by counterfeiters, the smaller the sampling required by authorities to detect these counterfeits, advantageously allowing hot lists to be created sooner rather than later, and circulated to investigators. The worst case for authorities is one-for-one copying only. If counterfeiters were able to do, and only did, one-for-one copying, authorities then would have much the same difficulty as in finding two and only two objects with the same serial number. However, with applicants' anti-counterfeit system in place, this too is possible given time.

Modifications And Other Embodiments

[0105] Complete product distribution and shipment history may also be associated with applicants' anti-counterfeit system computer, and augmented with the registration process, so that, for example, any products reported stolen (prior to being sold to the public) may be flagged and backtracked to apprehend the culprits when the stolen products are ultimately registered. Product distribution information, along with registration information, may also be useful for marketing, accounting, inventory, automation control, quality control, and other purposes.

[0106] Applicants' anti-counterfeit systems may be augmented and/or adapted for use to also detect product diversion, or gray marketing, as well as control problems with returns and seasonally packaged goods, product recalls for defects or tampered-with goods, etc.

[0107] For example, consider the Tylenol, or the more recent, Sudafed cyanide deaths. Had these medicine products been identified with an ID number, perhaps the individual ID numbers of the poisoned products might have been helpful to authorities (even if counterfeit was not involved). For example, had the murderer purchased the Sudafed at a retail store, poisoned the Sudafed, and then put the deadly medicine back on a retail shelf, but in a different retail store, this *modus operandi* might have been detected. Authorities might then reasonably have ruled out a manufacturing inside job. While batch numbers of the poisoned products were helpful to authorities, ID numbers would have provided more detailed information.

[0108] The U.S. Customs Service plays a large part in detecting counterfeit products at our nation's borders. In a preferred embodiment, applicants suggest that all companies should adopt uniform self-identifying bar code standards, of the type described in Table 1 (note Format F, 101, on Table 1, "Product or document 'Seal of Authenticity' service"), 1989, and should use common communication facilities and common counterfeit product computer system facilities. This would allow convenient means, for example, for U.S. Custom agents, as well as other investigators, to use the same bar code reading devices to check a variety of products for authenticity.

Table 1

Uniform Bar Code Standard Specifications Using Binary Coded Binary™, BCB™	
Format	General Format Description
A:000	Emulation of Code 39's character set of 43 alphanumeric characters, both without and with data identifiers as specified by FACT, including BCB efficiency and versatility enhancements.
B:001	Numerical information only, represented in Binary arithmetic.

Table 1 (continued)

Uniform Bar Code Standard Specifications Using Binary Coded Binary™, BCB™	
Format	General Format Description
C:010	Reserved for paper currency, including U.S. and foreign currency.
D:011	Alphanumeric, the full ASCII set of 128 (256?) characters, functions, etc., as specified by ANSI, using seven (eight?) BCB digit "words."
E:100	Emulation of all EAN & UPC symbols, but with enhancements.
F:101	Product or document "Seal of Authenticity" service.
G:110	User defined.
H:111	Other universal unified BCB bar code symbologies defined by a second set of three format bits which are adjacent to the first set of three format bits.

[0109] Products using these common standards and facilities might be identified with an associated "Seal of Authenticity." Also, some value may be had for example, if this Seal were a hologram or made with some other demanding printing technique, such as a detailed engraving. Or, as opposed to putting a "Seal of Authenticity" label on a product, the Seal may be printed along with other product packaging printing.

[0110] A "Seal of Authenticity" and/or the addition of a product return card to confirm authenticity might become part of a product's enhanced, and thus more desirable, image, as well as an integral part of a product's marketing strategy.

[0111] Another consideration here is the deterrent effect visible or invisible security ID number indicia may have, in possible association with a "Seal of Authenticity," on a would-be counterfeiter. There may be desirable effect, for example, to use prominently placed "Seals of Authenticity" on protected products, in association with advertising in strategically selected media of "ominous invisible high-tech fool-proof intellectual counterfeit-detecting bar coded security ID number indicium, positive protection with the absolute certainty of random counterfeit control that simply cannot be anticipated."

Dual Bar Code Mode of Operation

[0112] It may be efficient or otherwise desirable in some applications of applicants' invention, and for other purposes as well, to place two bar code symbols near each other. For example, it may be useful, where product packaging is printed with standard UPC bar code symbols, to place ID number indicia, such as shown in Fig. 2, on the same side of a product's packaging as the standard UPC bar code symbol, in convenient proximity thereto or association therewith, as shown in Fig. 3. For example, referring to Fig. 3, a truncated bar coded ID number is placed near the standard UPC bar code symbol, to the left of it with 3/8 inch of white space in-between.

[0113] Coincidentally, the UPC symbol shown to the right of the security ID number in Fig. 3 is a photo reproduction of an actual UPC symbol from a product called *Vistatector,* which is a pen-like device that can detect counterfeit currency or other counterfeit documents, a product of a New York City company, Vistatech Enterprises, Limited.

[0114] For example, locating two distinct bar code symbols near each other, such as a product's ID number and its UPC symbol, allows the possibility of an investigator reading the ID number in association with the UPC symbol, in the same reading or scanning operation, so that the product under scrutiny can be identified in accord with standard UPC product assignment coding, and individually identified for authenticity purposes with the ID number as described above.

[0115] In addition to convenience, this may allow smaller ID number indicia on packaging to be sufficient, since general product identification may be made via the UPC symbol, and/or this may be helpful by automatically informing authenticity apparatus what kind of product is being scrutinized.

[0116] It may be efficient or otherwise desirable in some applications of applicants' invention to make ID number indicia, such as shown in Fig. 2, or perhaps only the bar coded indicium of Fig. 2, substantially transparent, effectively invisible. Dolash et al.'s U.S. Pat. No. 4,983,817 describes how substantially transparent bar codes may be accurately read even though placed on top of visible printed text or even placed on top of a visible bar code symbol. For example, a bar coded ID number may be printed in invisible ink directly over a standard UPC symbol on a product's packaging, or in convenient proximity therewith.

[0117] If placed directly over a standard UPC symbol on a product's packaging, space dedicated on the packaging only for the ID number bar code symbol is not required, allowing more space for marketing purposes, without the distraction of another (visible) bar code. Another potential advantage is that both the UPC symbol and the bar coded ID number may then be scanned together, in one operation, automatically, as described below.

[0118] Or, as may be understood from Dolash et al., scanning is facilitated if an invisible bar code is printed on an otherwise blank space. If an invisible ID number were placed in an otherwise blank space, in convenient proximity with the UPC symbol, say, directly to the left of it, the invisible ID number in what appears to be a blank space would offer little distraction while allowing it to be conveniently scanned, although invisible, along with the UPC symbol, because bar code scanning operators could be taught to scan the blank space to the left of the UPC symbol. (For example, to understand this, imagine the bar coded ID number in Fig. 3 to the left of the UPC symbol to be invisible, so that the space the ID number now occupies appears blank to a person's eyes.)

[0119] An operator could be prompted by scanning apparatus if an invisible ID number has not been read while such apparatus is in certain selected modes of operation. For example, one mode of operation (referred to as a "dual mode setting") of bar code scanning apparatus may require that two different bar code symbols (i.e., each individual symbol is complete unto itself and each can be read separately) such as a visible UPC symbol and an invisible ID number (either superimposed over the visible UPC symbol or just placed near the visible UPC symbol) or a visible UPC symbol and a visible ID number (as shown in Fig. 3) be successfully read before indicating a reading operation has been completed.

[0120] Typically, for human operators, an audible beep and/or the lighting of an indicator light are often generated at the end of each bar code reading operation in order to indicate completion thereof. According to applicants' dual mode setting for reading bar codes, a signal indicating completion of the bar code reading operation would not be provided until both a visible UPC symbol and an invisible ID number (in one example) have been successfully read, i. e., a reading from one bar code symbol located near a second symbol is automatically delayed until the second is also read in the same reading operation or cycle (e.g., as ended with an associated beep).

[0121] The dual mode setting for reading bar codes may operate as follows: when a mode selector switch is set to the dual mode position, the switch could clamp the signal that would normally indicate the completion of one bar code reading until a second signal indicates the completion of a second reading of another bar code symbol. Then, with both signals present, each indicating a completed reading of a respective bar code symbol, the clamp may be lifted (unclamped) allowing the beep to sound and/or the indicator light to be lighted, thus indicating that both bar code symbols had been read in this dual mode setting. Other operations could also be accomplished before an indication of the end of a reading operation, e.g., price look-up, inventory list augmentation, authenticity check, date check, comparison to lists of ID numbers being sought by enforcement authorities, etc.)

[0122] The dual mode setting operation may be used with bar code reading apparatus even if human operators are not involved in the bar code reading operation. For example, a signal indicating completion would not be provided to associated circuits (as would normally be done after one bar code symbol was read) until two symbols were read.

[0123] The mode setting switch on bar code reading apparatus may select applicants' dual mode setting, and perhaps other settings as well, such as a single mode setting that anticipates a reading where only one bar code symbol per reading operation is present. For example, a setting where only the one UPC symbol will be read even if an invisible bar code is on top of it.

Automatic Dual Mode

[0124] In addition to the dual mode setting for bar code reading apparatus described above, it may be useful to also provide an "automatic dual mode setting" which would automatically detect whether one bar code symbol only was present in a relevant area, such as one side of a product being scanned, or whether two bar code symbols located near each other were present.

[0125] For example, if some supermarket products were protected against being counterfeited, as described above, with a transparent bar coded ID number superimposed over the standard UPC symbol, and some supermarket products were not protected, and therefore had only one UPC symbol present, applicants' automatic dual mode setting on check-out line scanning apparatus would allow reading both symbols when two are present on a protected product and one symbol when only one is present, no matter in what order various products are checked out, automatically, without undue delay.

[0126] Another example for use of applicants' automatic dual mode setting as described above would be for invisibly bar coded last-day-of-sale dates superimposed over the UPC code of supermarket products that require date stamping, like most milk or medicine products. Other products do not require any date stamping, like paper or plastic products.

[0127] Also, an invisible ID number symbol placed over a product's UPC symbol, for counterfeit detection purposes, can be used for detecting expired product. For example, the date of the last-day-of-sale for limited shelf-life products may be stored in a supermarket's computer in association with ID numbers. For example, the expiration date for ID

number bearing *Baby Safe Formula* product, 3/21/91, may be stored in the computer along with the information that the 3/21/91 expiration date applies to *Baby Safe Formula* with ID numbers (serial portion only) 1,000,000 to 1,001,000.

[0128] Then, when ID numbers from *Baby Safe Formula* are read at a check out counter and sent to the supermarket's computer, their expiration dates may be looked up, and/or authenticity may be checked (in real time or in a nocturnal batch processing operation, using the common communication and counterfeit product computer system facilities mentioned above) and/or various lists may be checked (price, inventory, stolen goods, counterfeit with repeated ID numbers, contaminated goods, etc.) etc.

[0129] If two bar code symbols were present, two bar code readings would be completed before the beep sounds and/or the indicator light lights, etc., indicating that both bar code symbols have been read. But if only one bar code symbol was present the beep would sound and/or the indicator light would light, etc., without undue delay, if any delay, after only one symbol has been read, i.e., one bar code symbol is automatically read without undue delay in the reading operation due to anticipation of another possible bar code symbol being near.

[0130] Also, it may be desirable to indicate whether one symbol or two different symbols have in fact been read. For example, when two bar code symbols are read, sound two beeps ("beep,beep" as opposed to "beep") and/or double blink the light repeatedly (blink,blink, pause, blink,blink, pause, blink,blink, ...) or light two lights or use colored lights, etc.

[0131] An automatic dual mode setting on bar code scanning apparatus is first described for one visible and one invisible bar code symbol, using a visible UPC symbol and an invisible ID number. For example, when reading UPC symbols in a visible nonluminescent frequency band, a bar code reading device could also sense for other bar code structure, as it senses for the UPC symbol. Sensing for this other bar code structure, of say, just a few bars and spaces, could be performed in a second invisible luminescent frequency band — that reflected by an invisible bar code. For example, Dolash et al.'s U.S. Pat. No. 4,983,817 describes dual bar code detection means for reading two differing frequency bands, comprising optical filters, collection optics, light detectors, etc.

[0132] If what appears to be part of an invisible bar code (e.g., a few bars and spaces) in this second band is in fact sensed in association with a UPC reading, the signal indicating completion of the bar code reading operation would not be provided until both the visible UPC symbol and the invisible ID number have been successfully read.

[0133] And *vice verse.* For example, if what appears to be part of a visible bar code in a nonluminescent frequency band is in fact sensed in association with an invisible reading in a second luminescent frequency band, the signal indicating completion of the invisible bar code reading operation would not be provided until both have been successfully read.

[0134] With additional provided means, a similar approach could be used if both bar codes were visible and placed near each other, as shown in Fig. 3. For example, if a few dark bars and a few light spaces are sensed in the proximity of another bar code symbol being read, the signal indicating completion of the bar code reading operation would not be provided until both visible bar code symbols have been successfully read.

[0135] There is a distinction, however, between sensing two bar code symbols when one (invisible) bar code is superimposed on the other, and reading two bar codes that are merely near each other (either both visible as shown in Fig. 3 or one visible next to one that is invisible). If a first symbol is superimposed on a second in a certain manner, so that it is not possible to miss scanning at least part of the first symbol before reading the second symbol completely, both symbols would always be read in the automatic dual mode setting of scanning apparatus. For example, the invisible superimposed bar code may be made at least as tall as the the UPC symbol underneath. and placed so that it spans at least part of this UPC symbol completely from top to bottom. Thus, at least part of the first invisible bar code symbol cannot be missed while reading the complete second visible symbol.

[0136] However, for example, referring to Fig. 3 where one visible bar code symbol is located next to another as shown: if during a reading operation with scanning apparatus set in automatic dual mode setting, scan lines came from the right and encountered the complete UPC symbol of Fig. 3 without going sufficiently past to also encounter part of the ID number symbol to the left (the normal required quiet zone for the bar code symbols described in these examples is understood to be 1/4 inch or less) a reading of only the UPC symbol may be provided along with a beep indicating completion of the reading operation even though two symbols are present next to each other and should be read together.

[0137] An example of a solution to this problem, where only one symbol is read when two are present near each other for reading together, is described. Scanning apparatus with automatic dual mode setting may be adjusted to work as follows: in automatic dual mode position the scan lines always go past the first bar code symbol encountered at least a fixed amount of, say effectively, 1/2 inch distance (this 1/2 inch being greater than what would otherwise be required for the quiet zone, as described). For example, referring back to Fig. 3, if during an automatic dual mode setting reading operation, scan lines came from the right and encountered the complete UPC symbol, the scan lines would continue at least 1/2 inch past the left end of the UPC symbol, traversing past the complete 3/8 inch space shown in Fig. 3, so that at least 1/8 inch part of the ID number symbol to the left of the UPC symbol is also encountered.

[0138] If no bars and spaces are encountered past the left end of the UPC symbol for the 1/2 inch of travel, apparatus proceeds on the basis that only the one UPC bar code symbol is present. For example, if scanning apparatus finds

1/2 inch of white space blank, the UPC code reading is provided and a beep would sound (once) and/or the indicator light would light (without blinking) after only one UPC symbol has been read, without undue pause.

[0139] In anticipation of the scanning 1/2 inch past the first bar code encountered requirement of apparatus with an automatic dual mode setting, printing specifications are made for putting two bar code symbols near each other as follows: the distance between two such symbols may be between 1/4 to 3/8 inch (3/8 inch is shown in Fig. 3) thereby insuring that the scan lines will always see at least 1/8 inch part of a second bar code symbol if present. Thus, in the automatic dual mode setting of scanning apparatus, when two symbols are near each other as specified, both will be read.

[0140] In order to avoid possible delay, care may also be taken when printing single bar code symbols (that may be read singly in an automatic dual mode setting) to either use a quiet zone of 1/2 inch minimum or not to use printing text or other material within 1/2 inch that might be interpreted as a few bars and spaces. If, for example, text were printed 1/4 inch from one UPC symbol, and this text were interpreted to be a few bars and spaces in automatic dual mode setting, delay may result from looking for another symbol (which is not present).

[0141] A scan line skewing effect is possible, similar to what may cause a short read [short reads may occur when a skewed scan line leaves or enters a symbol other than at the end(s) of the symbol] so that, still referring to Fig. 3, the ID number symbol may be missed by skewed scan lines reading the UPC symbol, or, in the example shown in Fig. 3, missed by high or low sufficiently horizontal scan lines because the ID number symbol is shown shorter (smaller) than the UPC symbol on both top and bottom.

[0142] To avoid this, the ID number symbol may be made taller than shown in Fig. 3, tall enough to extend above and below the UPC symbol, tall enough so that at least part of the top or bottom of the tall ID number symbol "catches" these skewed scan lines, to avoid the ID number symbol being missed altogether (only the part of the ID number symbol closest to the UPC symbol actually need be so tall). Or, the two symbols of Fig. 3 could be made the same height and placed in vertical alignment next to each other (i.e., both sitting on the same horizontal line and both rising to the same height therefrom) and bearer bars used across their tops and bottoms spanning the 1/4 inch to the 3/8 inch space in-between. As may be understood, the space between the two symbols cannot be too wide, i.e., greater than 3/8 inch in the above example.

[0143] Because scan lines may be skewed, the 1/2 inch distance that the scan lines go past the first bar code symbol encountered (as mentioned above) may need to be increased, perhaps to 3/4 or 1 inch, depending on other specifications, angles, etc. And, if the in-between space were 1/4 inch, not 3/8, the 1/2 inch distance may suffice.

[0144] Also, if accepted standard conventions regarding the quiet zones of two symbols that are to be located near each other are modified, then part of an adjacent symbol, such as a few bars and spaces, might be handled as described above, and the two symbols read even though they are in what might otherwise be each other's quiet zone.

[0145] If scanning lines encounter only one bar code symbol in the automatic dual mode setting position of scanning apparatus notwithstanding the above possible superimpositions, distances, adjustments, specifications, etc., said one bar code symbol would be read and the beep would sound (once) and/or the indicator light would light (without blinking) after only one symbol has been read, with no undue delay, if any delay at all, in the reading operation due to anticipation of another possible bar code symbol being near.

[0146] Some delay might be caused and/or operator time wasted, for example, if a bar code scanning operator had to inform his apparatus whether one or two bar code symbols were to be read in a given reading operation, or, for example, if apparatus had to scan an area somewhat exhaustively to determine if one or two distinct bar code symbols were present before coming to the end of a given reading operation, when only one was present.

[0147] According to applicants' invention, another method may be used to automatically determine whether only one bar code symbol was present in a relevant area being scanned, or whether two bar code symbols located near each other were present. Referring yet again to Fig. 3 by way of example, there is one ID number bar code symbol to the left near one UPC bar code symbol. For example, in a selected automatic dual mode of operation, bar code scanning apparatus could always sense for the presence of a UPC symbol, and when a UPC symbol is read. look up this particular UPC symbol in a computer listing (the price associated with each UPC symbol, for example, for milk, medicine and paper products, is looked up in a computer) to check the "invisible bar code also?" flag which, depending if this flag is on or off, automatically informs apparatus whether or not another bar code should also be read along with this UPC symbol. In other words, the computer stores the information for each UPC code that may be read, as to whether or not another bar code symbol should be present and should also be read. Also, more than one flag could be used, in order to inform, e.g., which other particular bar code symbol(s) should be present and should be read, or, if more than one, which one(s) should be read, etc.

[0148] Another way of automatically informing bar code scanning apparatus whether one or two bar code symbols should be read in a given reading operation is, referring back to Table 1 on page 31, to assign another distinct format, e.g., Format X (not shown). Convention for using this format is that Format X BCB bar code symbols also require that, for example, whenever a BCB Format X symbol is read, a Code 39 symbol located near should also be read in a given reading operation. In other words, the particular bar code symbol itself may, by convention, inform whether one or two

bar code symbols should be read in a given reading operation.

[0149] Another example of this aspect of applicants' invention, with UPC convention, would be to assign one or more UPC Number System Characters, e.g., 1, 6, 7, 8 or 9, which were "Reserved for uses unidentified at this time," i.e., reserved when UPC conventions were adopted, to inform whether one UPC symbol or one UPC symbol and at least another bar code symbol should also be read in a given reading operation.

[0150] Certain changes and modifications of the embodiments of the invention disclosed herein will be readily apparent to those skilled in the art. It is the applicants' intention to cover by the claims all such uses of the invention and all those changes and modifications which could be made to the embodiments of the invention as herein chosen for the purpose of disclosure, without departing from the scope of the invention as defined by the appended claims.

Claims

1. A method for identifying unauthorized objects comprising:

on at least one less accessible location of each authorized object associating identifying information therewith which includes at least two distinct randomly selected portions;
on at least one other more accessible location of each authorized object associating said identifying information therewith but omitting at least one said distinct portion;
storing said identifying information with said at least two distinct portions aside from said associations with said authorized objects;
reading identifying information from at least one of said locations associated with an object being checked for authenticity;
comparing said read information with corresponding said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

2. A method for identifying unauthorized objects comprising:

on at least one less accessible location of each authorized object associating identifying information therewith which includes at least two distinct randomly selected portions;
in at least one other more accessible location of each authorized object associating said identifying information therewith but omitting at least one said distinct portion;
storing said information with said at least two distinct portions aside from said associations with said authorized objects;
reading identifying information from said one other more accessible location associated with an object being check for authenticity;
comparing said read information from said one other more accessible location with corresponding said stored information to detect discrepancy therebetween, whereby an unauthorized object is identified;
reading identifying information including said at least two distinct portions from said at least one less accessible location associated with an object being checked for authenticity;
comparing said read information from said at least one less accessible location with corresponding portions of said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

3. A method for identifying unauthorized objects with outer covering, such as products with packaging, comprising:

on at least one location inside said covering of each authorized object associating identifying information therewith which includes at least two distinct randomly selected portions;
on at least one location on the outside of said covering of each authorized object associating said identifying information therewith but omitting at least one said distinct portion;
storing said information with said at least two distinct portions aside from said associations with said authorized objects;
reading identifying information from at least one of said locations associated with an object being checked for authenticity;
comparing said read information with corresponding said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

4. A method for identifying unauthorized objects with outer covering, such as products with packaging, comprising:

on at least one location inside said covering of each authorized object associating identifying information therewith which includes at least two distinct randomly selected portions;
on at least one location on the outside of said covering of each authorized object associating said identifying information therewith but omitting at least one said distinct portion;
storing said information with said at least two distinct portions aside from said associations with said authorized objects;
reading identifying information from at least one location on the outside of an object being checked for authenticity;
comparing said read information from said outside location with corresponding said stored information to detect discrepancy therebetween, whereby an unauthorized object is identified;
reading identifying information including at least two said distinct portions from at least one inside location of an object being checked for authenticity;
comparing said read information from said inside location with corresponding said stored information to detect one or more discrepancies therebetween, whereby an unauthorized object is identified.

5. A method of designating an object as authorized comprising:

randomly selecting at least two distinct digits;
storing said two distinct digits with said authorized object's serial number; and,
associating said serial number and one distinct digit of said two distinct digits with said object on the outer surface thereof; and,
associating said serial number and said two distinct digits with said object inside the outer surface thereof.

6. A method of designating an object as authorized comprising:

randomly selecting at least two djstinct digits;
storing said at least two distinct digits along with an authorized object's serial number as a complete authorized identifying number; and,
associating said serial number and one distinct digit of said at least two distinct digits with said object on the outer surface thereof.

7. The method according to claim 6 wherein said serial number and said two distinct digits are located inside said object's outer surface.

8. The method according to claim 7 wherein said serial number and said two distinct digits located inside said object's outer surface are associated with a return card for said object.

9. A system for identifying an unauthorized object from a set of authorized objects, each authorized object of said set having identifying information associated therewith of which a portion has been calculated using an algorithm dependent on a randomly selected number, the system comprising:

means for securely storing said randomly-selected numbers at a single location only;
means for reading identifying information from an object;
means coupled to receive said information read from said object for at least temporarily storing that information; and
means for automatically detecting when information read from any object includes a different said portion than that calculated using said algorithm, whereby an unauthorized object is identified.

10. The system according to claim 9,also comprising means for automatically erasing said portion calculated using said algorithm after said association with said authorized object.

11. A method for identifying unauthorized objects comprising:

associating with each authorized object identifying information which includes a plurality of randomly selected portions, at least one said randomly selected portion being concealed in a given condition of said objects and at least one said randomly selected portion being visible in said given condition of said object;
storing said information aside from said association with said authorized objects;
reading said information from an object being checked for authenticity; and

comparing said read information with said stored information to detect discrepancy therebetween, whereby an unauthorized object is identified.

Patentansprüche

1. Verfahren zum Identifizieren von nicht autorisierten Objekten, umfassend die folgenden Schritte:

an wenigstens einer weniger zugänglichen Stelle jedes autorisierten Objekts, Assoziieren von Identifikationsinformation damit, die wenigstens zwei unterschiedliche zufällig gewählte Abschnitte umfasst;

an wenigstens einer anderen mehr zugänglichen Stelle jedes autorisierten Objekts, Assoziieren der Identifikationsinformation damit, aber Weglassen wenigstens eines unterschiedlichen Abschnitts;

Speichern der Identifikationsinformation mit den wenigstens zwei unterschiedlichen Abschnitten an der Seite von den Assoziationen mit den autorisierten Objekten;

Lesen von Identifikationsinformation von wenigstens einer der Stellen, die mit einem Objekt assoziiert ist, welches für eine Authentizität überprüft wird; und

Vergleichen der gelesenen Information mit einer entsprechenden gespeicherten Information, um eine oder mehrere Diskrepanzen dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird.

2. Verfahren zum Identifizieren von nicht autorisierten Objekten, umfassend:

an wenigstens einer weniger zugänglichen Stelle jedes autorisierten Objekts, Assoziieren von Identifikationsinformation damit, die wenigstens zwei unterschiedliche zufällig gewählte Abschnitte umfasst;

an wenigstens einer anderen mehr zugänglichen Stelle jedes autorisierten Objekts, Assoziieren der Identifikationsinformation damit, aber Weglassen wenigstens eines unterschiedlichen Abschnitts;

Speichern der Information mit den wenigstens zwei unterschiedlichen Abschnitten an der Seite von den Assoziationen mit den autorisierten Objekten;

Lesen von Identifikationsinformation von der einen anderen mehr zugänglichen Stelle, die mit einem Objekt assoziiert wird, das für eine Authentizität überprüft wird;

Vergleichen der gelesenen Information von der einen anderen mehr zugänglichen Stelle mit der entsprechenden gespeicherten Information, um eine Diskrepanz dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird;

Lesen von Identifikationsinformation, die die wenigstens zwei unterschiedlichen Abschnitte umfasst, von der wenigstens einen weniger zugänglichen Stelle, die mit einem Objekt assoziiert ist, welches für eine Authentizität überprüft wird; und

Vergleichen der gelesenen Information von der wenigstens einen weniger zugänglichen Stelle mit entsprechenden Abschnitten der gespeicherten Information, um eine oder mehrere Diskrepanzen dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird.

3. Verfahren zum Identifizieren von nicht autorisierten Objekten mit einer äußeren Abdeckung, wie Produkte mit einer Verpackung, umfassend die folgenden Schritte:

an wenigstens einer Stelle innerhalb der Abdeckung jedes autorisierten Objekts, Assoziieren von Identifikationsinformation damit, die wenigstens zwei unterschiedliche zufällig gewählte Abschnitte umfasst;

an wenigstens einer Stelle außerhalb von der Abdeckung jedes autorisierten Objekts, Assoziieren der Identifikationsinformation damit, aber Weglassen wenigstens eines unterschiedlichen Abschnitts;

Speichern der Information mit den wenigstens zwei unterschiedlichen Abschnitten an der Seite von den Assoziationen mit den autorisierten Objekten;

Lesen von Identifikationsinformation von wenigstens einer der Stellen, die mit einem Objekt assoziiert ist, welches für eine Authentizität überprüft wird; und

Vergleichen der gelesenen Information mit der entsprechenden gespeicherten Information, um eine oder mehrere Diskrepanzen dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird.

4. Verfahren zum Identifizieren von nicht autorisierten Objekten mit einer äußeren Abdeckung, wie Produkte mit einer Verpackung, umfassend:

an wenigstens einer Stelle innerhalb der Abdeckung jedes autorisierten Objekts, Assoziieren von Identifikationsinformation damit, die wenigstens zwei unterschiedliche zufällig gewählte Abschnitte umfasst;

an wenigstens einer Stelle außerhalb der Abdeckung jedes autorisierten Objekts, Assoziieren der Identifikationsinformation damit, aber Weglassen wenigstens eines unterschiedlichen Abschnitts;

Speichern der Information mit den wenigstens zwei unterschiedlichen Abschnitten an der Seite von den Assoziationen mit den autorisierten Objekten;

Lesen von Identifikationsinformation von wenigstens einer Stelle außerhalb eines Objekts, welches für eine Authentizität überprüft wird;

Vergleichen der gelesenen Information von der äußeren Stelle mit der entsprechenden gespeicherten Information, um eine Diskrepanz dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird;

Lesen von Identifikationsinformation, die die wenigstens zwei unterschiedlichen Abschnitte umfasst, von wenigstens einer inneren Stelle eines Objekts, das für eine Authentizität überprüft wird; und

Vergleichen der gelesenen Information von der inneren Stelle mit der entsprechenden gespeicherten Information, um ein oder mehrere Diskrepanzen dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird.

5. Verfahren zum Bestimmen eines Objekts als autorisiert, umfassend:

zufälliges Wählen von wenigstens zwei unterschiedlichen Zahlzeichen;

Speichern der zwei unterschiedlichen Zahlzeichen mit der Seriennummer des autorisierten Objekts; und

Assoziieren der Seriennummer und eines unterschiedlichen Zahlzeichens der zwei unterschiedlichen Zahlzeichen mit dem Objekt auf der äußeren Oberfläche davon; und

Assoziieren der Seriennummer und der zwei unterschiedlichen Zahlzeichen mit dem Objekt innerhalb der äußeren Oberfläche davon.

6. Verfahren zum Bestimmen eines Objekts als autorisiert, umfassend die folgenden Schritte:

zufälliges Wählen von wenigstens zwei unterschiedlichen Zahlzeichen;

Speichern der wenigstens zwei unterschiedlichen Zahlzeichen zusammen mit einer Seriennummer eines autorisierten Objekts als eine vollständige autorisierte Identifikationszahl; und

Assoziieren der Seriennummer und eines unterschiedlichen Zahlzeichens der wenigstens zwei unterschiedlichen Zahlzeichen mit dem Objekt auf der äußeren Oberfläche davon.

7. Verfahren nach Anspruch 6, wobei die Seriennummer und die zwei unterschiedlichen Zahlzeichen innerhalb der äußeren Oberfläche des Objekts angeordnet sind.

8. Verfahren nach Anspruch 7, wobei die Seriennummer und die zwei unterschiedlichen Zahlzeichen, die innerhalb der äußeren Oberfläche des Objekts angeordnet sind, mit einer Rückgabekarte für das Objekt assoziiert werden.

9. System zum Identifizieren eines nicht autorisierten Objekts aus einem Satz von autorisierten Objekten, wobei jedes autorisierte Objekt des Satzes eine damit assoziierte Identifikationsinformation aufweist, wobei ein Abschnitt davon unter Verwendung eines Algorithmus in Abhängigkeit von einer zufällig gewählten Zahl berechnet worden ist, wobei das System umfasst:

eine Einrichtung zum gesicherten Speichern der zufällig gewählten Zahlen an nur einer einzelnen Stelle;

eine Einrichtung zum Lesen von Identifikationsinformation von einem Objekt;

eine Einrichtung, die gekoppelt ist, um die von dem Objekt gelesene Information zu empfangen, um wenigstens vorübergehend diese Information zu speichern; und

eine Einrichtung zum automatischen Erfassen, wenn eine von irgendeinem Objekt gelesene Information einen anderen besagten Abschnitt als denjenigen, der unter Verwendung des Algorithmus berechnet wird, umfasst, wodurch ein nicht autorisiertes Objekt identifiziert wird.

10. System nach Anspruch 9, ferner umfassend eine Einrichtung zum automatischen Löschen des Abschnitts, der unter Verwendung des Algorithmus berechnet wird, nach der Assoziation mit dem autorisierten Objekt.

11. Verfahren zum Identifizieren von nicht autorisierten Objekten, umfassend die folgenden Schritte:

Assoziieren von Identifikationsinformation, die eine Vielzahl von zufällig gewählten Abschnitten umfasst, mit jedem autorisiertem Objekt, wobei wenigstens einer der zufällig gewählten Abschnitte in einer gegebenen Bedingung der Objekte verdeckt ist und wenigstens einer der zufällig gewählten Abschnitte in der gegebenen Bedingung des Objekts sichtbar ist;
Speichern der Information an der Seite von der Assoziation mit den autorisierten Objekten;
Lesen der Information von einem Objekt, welches für eine Authentizität überprüft wird; und
Vergleichen der gelesenen Information mit der gespeicherten Information, um eine Diskrepanz dazwischen zu erfassen, wodurch ein nicht autorisiertes Objekt identifiziert wird.

Revendications

1. Un procédé pour identifier des objets non autorisés, comprenant les étapes suivantes :

sur au moins un emplacement moins accessible de chaque objet autorisé, on associe à celui-ci une information d'identification qui comprend au moins deux parties distinctes sélectionnées de manière aléatoire;

sur au moins un autre emplacement plus accessible de chaque objet autorisé, on associe à celui-ci l'information d'identification, mais en omettant au moins l'une des parties distinctes;

on stocke l'information d'identification avec les aux moins deux parties distinctes, séparément desdites associations avec les objets autorisés;

on lit l'information d'identification à partir de l'un au moins des emplacements associés à un objet dont on contrôle l'authenticité;

on compare l'information lue avec l'information stockée correspondante, pour détecter une ou plusieurs discordances entre elles, grâce à quoi un objet non autorisé est identifié.

2. Un procédé pour identifier des objets non autorisés, comprenant les étapes suivantes :

sur au moins un emplacement moins accessible de chaque objet autorisé, on associe à celui-ci une information d'identification qui comprend au moins deux parties distinctes sélectionnées de façon aléatoire;

dans au moins un autre emplacement plus accessible de chaque objet autorisé, on associe à celui-ci l'information d'identification, mais en omettant l'une au moins des parties distinctes;

on stocke ladite information avec les aux moins deux parties distinctes, séparément desdites associations avec les objets autorisés;

on lit l'information d'identification à partir de l'autre emplacement plus accessible associé à un objet dont on contrôle l'authenticité;

on compare l'information lue provenant de l'autre emplacement plus accessible avec l'information stockée correspondante, pour détecter des discordances entre elles, grâce à quoi un objet non autorisé est identifié;

on lit l'information d'identification incluant les aux moins deux parties distinctes, à partir de l'au moins un emplacement moins accessible associé à un objet dont on contrôle l'authenticité;

on compare l'information lue provenant de l'au moins un emplacement moins accessible avec des parties correspondantes de l'information stockée, pour détecter une ou plusieurs discordances entre elles, grâce à quoi un objet non autorisé est identifié.

3. Un procédé pour identifier des objets non autorisés avec une enveloppe extérieure, tels que des produits avec emballage, comprenant les étapes suivantes :

sur au moins un emplacement à l'intérieur de l'enveloppe de chaque objet autorisé, on associe à celui-ci une information d'identification qui comprend au moins deux parties distinctes sélectionnées de façon aléatoire;

sur au moins un emplacement sur l'extérieur de l'enveloppe de chaque objet autorisé, on associe à celui-ci l'information d'identification, mais en omettant l'une au moins des parties distinctes;

on stocke ladite information avec les aux moins deux parties distinctes, séparément desdites associations avec les objets autorisés;

on lit l'information d'identification à partir de l'un au moins des emplacements associés à un objet dont on contrôle l'authenticité;

on compare l'information lue avec l'information stockée correspondante pour détecter une ou plusieurs discordances entre elles, grâce à quoi un objet non autorisé est identifié.

4. Un procédé pour identifier des objets non autorisés avec une enveloppe extérieure, tels que des produits avec emballage, comprenant les étapes suivantes :

sur au moins un emplacement à l'intérieur de l'enveloppe de chaque objet autorisé, on associe à celui-ci une information d'identification qui comprend au moins deux parties distinctes sélectionnées de façon aléatoire;

sur au moins un emplacement sur l'extérieur de l'enveloppe de chaque objet autorisé, on associe à celui-ci l'information d'identification, mais en omettant l'une au moins des parties distinctes;

on stocke ladite information avec les aux moins deux parties distinctes, séparément desdites associations avec les objets autorisés;

on lit l'information d'identification à partir d'au moins un emplacement sur l'extérieur d'un objet dont on contrôle l'authenticité;

on compare l'information lue à partir de l'emplacement extérieur avec l'information stockée correspondante, pour détecter une discordance entre elles, grâce à quoi un objet non autorisé est identifié;

on lit l'information d'identification comprenant les aux moins deux parties distinctes, à partir d'au moins un emplacement intérieur d'un objet dont on contrôle l'authenticité;

on compare l'information lue à partir de l'emplacement intérieur avec l'information stockée correspondante, pour détecter une ou plusieurs discordances entre elles, grâce à quoi un objet non autorisé est identifié.

5. Un procédé de désignation d'un objet comme étant autorisé, comprenant les étapes suivantes :

on sélectionne de façon aléatoire au moins deux chiffres distincts;

on stocke ces deux chiffres distincts avec le numéro de série de l'objet autorisé; et

on associe à l'objet, sur la surface extérieure de celui-ci, le numéro de série et un chiffre distinct parmi les deux chiffres distincts; et,

on associe à l'objet, à l'intérieur de sa surface extérieure, le numéro de série et les deux chiffres distincts.

6. Un procédé de désignation d'un objet comme étant autorisé, comprenant les étapes suivantes :

on sélectionne de façon aléatoire au moins deux chiffres distincts;

on stocke ces au moins deux chiffres distincts conjointement à un numéro de série d'un objet autorisé, sous la forme d'un numéro d'identification autorisé complet; et

on associe à l'objet, sur la surface extérieure de celui-ci, le numéro de série et un chiffre distinct parmi les au moins deux chiffres distincts.

7. Le procédé selon la revendication 6, dans lequel le numéro de série et les deux chiffres distincts sont placés à l'intérieur de la surface extérieure de l'objet.

8. Le procédé selon la revendication 7, dans lequel le numéro de série et les deux chiffres distincts placés à l'intérieur de la surface extérieure de l'objet sont associés à une carte de retour pour l'objet.

9. Un système pour identifier un objet non autorisé parmi un ensemble d'objets autorisés, chaque objet autorisé de l'ensemble étant associé à une information d'identification dont une partie a été calculée en utilisant un algorithme qui dépend d'un nombre sélectionné de façon aléatoire, le système comprenant :

des moyens pour stocker de façon sûre les nombres sélectionnés de façon aléatoire uniquement à un seul emplacement;

des moyens pour lire une information d'identification à partir d'un objet;

des moyens couplés pour recevoir l'information lue à partir de l'objet, pour stocker au moins temporairement cette information; et

des moyens pour détecter automatiquement le moment auquel l'information lue sur un objet quelconque comprend une partie précitée différente de celle calculée en utilisant l'algorithme, grâce à quoi un objet non autorisé est identifié.

10. Le système selon la revendication 9, comprenant également des moyens pour effacer automatiquement la partie calculée en utilisant l'algorithme, après l'association avec l'objet autorisé.

11. Un procédé pour identifier des objets non autorisés, comprenant les étapes suivantes :

on associe à chaque objet autorisé une information d'identification qui comprend une multiplicité de parties sélectionnées de façon aléatoire, l'une au moins des parties sélectionnées de façon aléatoire étant cachée dans une condition donnée des objets, et l'une au moins des parties sélectionnées de façon aléatoire étant visible dans cette condition donnée de l'objet;

on stocke cette information séparément de ladite association avec les objets autorisés;

on lit cette information sur un objet dont on contrôle l'authenticité; et

on compare l'information lue avec l'information stockée pour détecter une discordance entre elles, grâce à quoi un objet non autorisé est identifié.

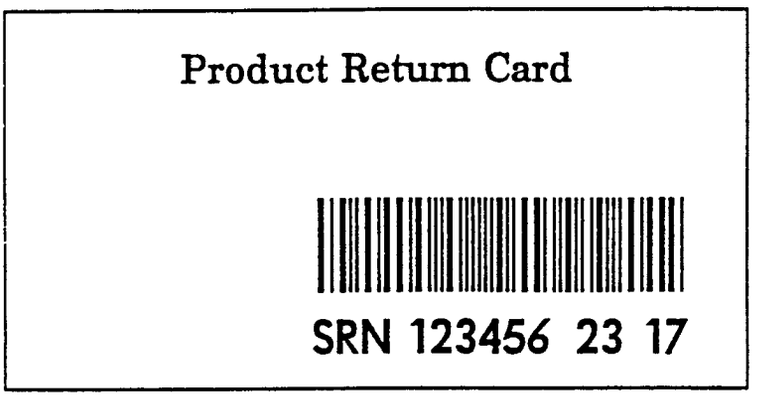
Product Return Card
SRN 123456 23 17

Fig. 1

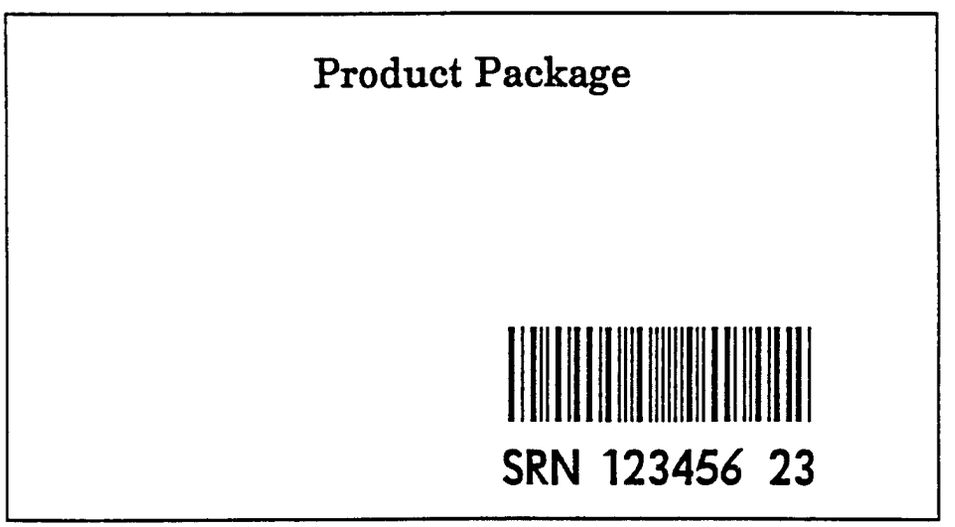
Product Package
SRN 123456 23

Fig. 2

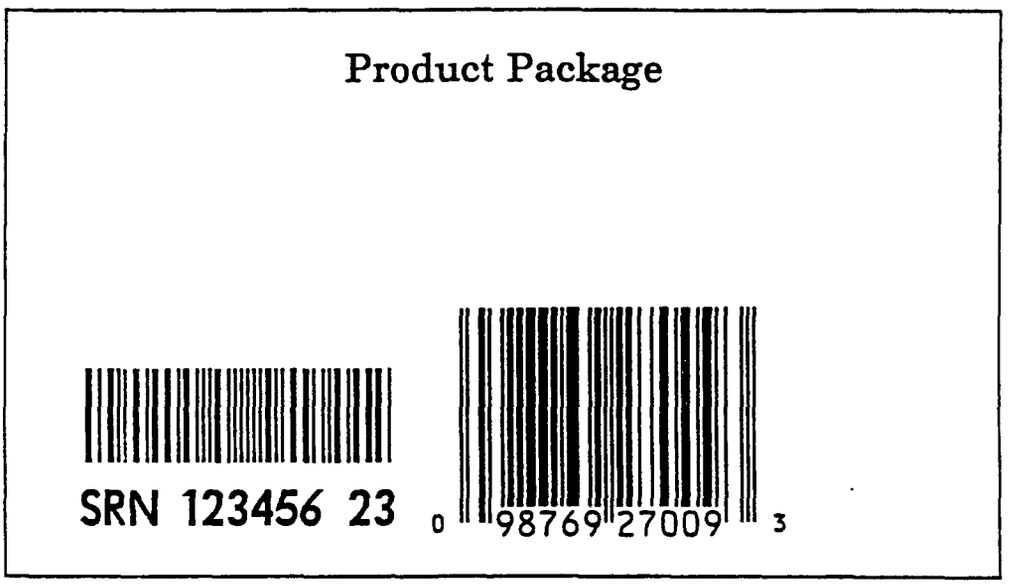

Fig. 3