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

(11) EP 0 772 929 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.09.2006 Bulletin 2006/36

(21) Application number: **95928140.3**

(22) Date of filing: **26.07.1995**

(51) Int Cl.:
G07C 9/00 *(2006.01)* ***G07F 7/08*** *(2006.01)*
H04L 9/00 *(2006.01)*

(86) International application number:
PCT/US1995/009397

(87) International publication number:
WO 1996/003821 (08.02.1996 Gazette 1996/07)

(54) **METHODS AND SYSTEMS FOR CREATING AND AUTHENTICATING UNALTERABLE SELF-VERIFYING ARTICLES**

VERFAHREN UND SYSTEME ZUR ERZEUGUNG UND AUTHENTIFIZIERUNG UNVERÄNDERBARER SELBSTÜBERPRÜFENDER ARTIKEL

PROCEDES ET SYSTEMES DE CREATION ET D'AUTHENTIFICATION D'ARTICLES INALTERABLES A AUTO-VERIFICATION

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **26.07.1994 US 280785**

(43) Date of publication of application:
14.05.1997 Bulletin 1997/20

(73) Proprietor: **Siemens Energy and Automation, Inc.**
Alpharetta GA 30005 (US)

(72) Inventor: **PRIDDY, Dennis, G.**
Clearwater, FL 34630 (US)

(74) Representative: **Barnfather, Karl Jon et al**
Withers & Rogers LLP
Goldings House,
2 Hays Lane
London SE1 2HW (GB)

(56) References cited:
EP-A- 0 440 814
EP-A- 0 486 973
EP-A- 0 599 558
GB-A- 1 369 537
GB-A- 2 248 360
US-A- 3 956 615
US-A- 4 004 089
US-A- 4 016 404
US-A- 4 179 686
US-A- 5 241 600
US-A- 5 324 923

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 0 772 929 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates in general to encoding methods and systems, and in particular to methods, systems and articles of manufacture for creating and authenticating self-verifying articles.

BACKGROUND OF THE INVENTION

[0002] Modern life requires that individual identification and document authenticity be quickly, conveniently and reliably verified. The necessity for both individual and document verification arises in almost every commercial transaction.

[0003] Additionally, the necessity for individual identification arises in both social and governmental settings with ever increasing frequency.

[0004] Commercial transactions requiring both document verification and individual identification include credit card, calling card, automatic teller machine ("ATM") and similar transactions, as well as other daily commercial transactions such as check cashing. For example, when a check is presented to a bank for payment, the bank is required to verify the authenticity of the check writer's signature (called the endorsement) and that there is enough money in the checking account to cover the check.

[0005] Authenticity of the endorsement is determined by comparing the signature appearing upon the check with a signature sample of the check writer on file with the bank. A reasonably good forgery of the endorsement might enable an unauthorized person to illegally cash the check.

[0006] Alternatively, in non-commercial settings, identification issues often arise in the context of security. For example, common apartment and office building security systems require that anyone wishing to enter the building "sign in" in front of a security guard, and often, to present the guard with a previously issued personal identification document which authorizes access to the building. The security guard is required to exercise his best personal judgment to determine that the identification document is authentic and that the person presenting it is the person identified on the identification document. In such circumstances, and understandably so, a security guard may be deceived by a person who is correctly identified on a forged or altered identification document. In the governmental context, it is a requirement in many countries that citizens carry personal identification papers in public to be produced for review upon request by appropriate authorities.

[0007] For example, private individuals are required to present to the police personal identification, such as a driver's license, at the scene of a traffic accident or when stopped for a traffic violation. Additionally, personal identification documents are required for admittance to voting polls, and when crossing international boundaries and/or importing or exporting goods.

[0008] Accordingly, a pronounced need exists for unalterable self verifying personal, commercial and governmental identification cards, papers, documents, labels, packaging and other similar articles. For the purposes of this patent document, an article shall be defined as any item having a surface, which may include a substrate, to which data may be fixed. As used herein, the term fixed shall mean one or more of the following, but is not limited to, attached, imprinted, adhered, etched, scratched, painted, printed, peened, embedded, machined, drilled, stamped, or otherwise imaged.

[0009] One current solution requires the use of biometric information that is stored in a memory device carried by an individual. The term biometric information refers to a characteristic personal to an individual, such as a signature, a finger print or a picture, for example. A sample of biometric information to be used is obtained from the person at an "encodation" site where the memory device is programmed under secure conditions. The sample is formed into a code by conventional encoding techniques. The sample may be obtained by having the person place a hand, eye, face or other unique physical feature upon a scanning input device. The scanned information is then encoded to form a code which is subsequently stored to an alterable, portable memory device (i.e., magnetic strips, electronic or optical memory cards, floppy disks, etc.).

[0010] The portable memory device is issued to the person. When the person's identity needs to be verified, the person presents the portable memory device at a "remote access/decodation" site where identification verification is to occur, and the information contained within the portable memory device is read from memory.

[0011] Another sample of biometric information is then obtained by the person again placing a particular physical feature upon the input scanning device. The read code and the just sampled biometric information are compared by a machine to determine authenticity.

[0012] In this regard, the read code may be decoded, e.g., using a process that reverses the encodation performed previously, or the sample information encoded, e.g., using the same encoding process used at the encryption site, to make the comparison. Because this method requires a processing system for performing data encoding and/or decoding, complex opto-electric hardware at every encodation and remote access site, and a memory device for each person, this solution is exceedingly expensive.

[0013] In EP 0599558 there is disclosed use of an identification card and method and apparatus for producing and authenticating such an identification card. Identity, Status or characteristics are scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which

is incorporated into one portion of the identification card. The image is also printed or otherwise embodied onto another portion of the identification card. A text message maybe appended to the signal before it is encrypted and also printed as plain text on the identification card. In one embodiment the signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. This key maybe changed from time to time to increase security. To facilitate authentication the corresponding decryption key is encrypted with another key and incorporated on the card. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. The card may then be authenticated by comparison of the displayed representation of the image and the displayed text message with the image and text message printed on the card.

[0014] It is therefore an object of the present invention to provide an unalterable code, for use on an article, which contains biometric identification information personal to the authorized bearer of the article.

[0015] Another object of the present invention is to provide methods and systems for inexpensively, accurately and efficiently producing unalterable self-verifying personal and commercial articles.

[0016] A further object of the present invention is to provide methods and systems for accurately, efficiently and inexpensively authenticating presented self-verifying articles.

[0017] A still further object of the present invention is to provide methods and systems for verifying the authenticity of self-verifying articles presented at remote access sites which do not require expensive verification equipment, such as physical-trait-scanning input devices, or the inconvenience of a communication channel to a central location.

SUMMARY OF THE INVENTION

[0018] The invention is directed to a self-verifying article which contains an encoded machine-readable data set which includes recipient-specific biometric data. Self-verifying articles include, for example, commercial instruments (i.e., notes, drafts, checks, bearer paper, etc.), transaction cards (i.e., ATM cards, calling cards, credit cards, etc.), personal identification documents (i.e., driver's licenses, government benefit cards, passports, personal identification papers, etc.) and labels affixed to package surfaces, including for example identification of the package owner or sender, which may be used for verifying imported goods by customs agents. A subset of, or the whole of, the biometric data set may be, for example, a graphic image of a personal characteristic considered unique to a particular individual, such as, for example, a fingerprint, a retinal scan, a photo, a signature, etc., or some combination of the foregoing, is encoded to generate a machine readable data set. This article is preferably a low cost article, of paper or plastic, but may be any substrate, and the machine-readable data set is preferably fixed upon or in the article. The article also may, but need not, contain a human readable version of the biometric data set.

[0019] The object of the invention is attained by the features of the independent claims respectively. Preferred embodiments of the invention are subject-mather of the respective dependent claims.

[0020] In one embodiment of the invention, the encoded machine readable data set is fixed upon the article in a manner which is neither comprehensible, nor detectable, by the human-eye, unless assisted by a suitably arranged reading device. For example, a check, or any other article for that matter, has fixed thereon a machine readable data set including the authorized user's signature. Thus, a would be forger would not have a sample of an authorized signature to copy. A comparison of the user's signature with the decoded signature permits verification at the site of use.

[0021] In another embodiment, a human-readable textual data set also appears on the article, optionally with selected subsets of the textual data set also being encoded and concatenated, interleaved, etc. with the encoded biometric data set. For the purpose of this patent document, a textual data set comprises all data which is not biometric data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings in which like numbers designate like parts, and in which.

FIG. 1A illustrates a functional block diagram of a system for producing a self-verifying article in accordance with the principles of the present invention;

FIG. 1B illustrates an isometric view of the processing system set forth in FIG.1A;

FIG. 1C illustrates a block diagram of a processing unit and a memory storage device;

FIG. 2A illustrates a functional block diagram of a system for verifying the authenticity of a received self-verifying article in accordance with the principles of the present invention;

FIG. 2B illustrates an isometric view of the remote access site processing system set forth in FIG. 2A;

FIG. 3 illustrates a machine-readable binary coded matrix;

FIGS. 4A and 4B illustrate flow diagrams for producing an unalterable self-verifying article in accordance with the embodiment illustrated in FIG. 1A; and

FIG. 5 illustrates a flow diagram for verifying the authenticity of a received self-verifying article in accordance with the embodiment illustrated in FIG. 2A.

DETAILED DESCRIPTION OF THE INVENTION

[0023] FIG. 1A illustrates a functional diagram of a system for producing a self-verifying article in accordance with the present invention. The system includes an input data set 100, which includes a biometric data set 101 and an optional textual data set 102, an article 10, a processing system 103 and a self verifying article 104. As previously introduced, data set 100 is comprised of recipient specific data. Biometric data set 101 may include one or more physical traits personal to the potential article recipient (i.e., photo, retinal scan, finger print, signature, etc.), while textual data set 102, which is optionally included in input data set 100, may include one or more textual attributes (i.e., name, address, height/weight, eye color, etc.).

[0024] Processing system 103 is operable to produce self verifying article 104 by generating a unique machine-readable data set for fixing upon article 10.

[0025] Processing system 103 includes input means, processing means, output means and article producing means. The input means are for receiving input data set 100 and article 10. The processing means are for validating input data set 100, both syntactically and semantically, and encoding selected subsets of biometric data set 101, and, optionally, selected portions of textual data set 102 (optionally, the data to be encoded may first be encrypted, if desired). The output means are for transmitting a validated and encoded data set, along with the selected subsets of biometric data set 101, and optionally with the textual data set 102, to the article producing means. The article producing means are for fixing the validated and encoded data set, and for optionally fixing the selected subsets of biometric data set 101 and optionally textual data set 102, to article 10, thereby producing self-verifying article 104.

[0026] In the preferred embodiment, processing system 103 ensures data integrity by encoding all selected biometric and textual data subsets into a compact unalterable machine-readable data set, and subsequently, configuring the machine-readable data set as one or more matrices. If preferred, the machine-readable data set may be divided into two or more individual segments, which segments may then be incorporated into two or more two dimensional machine-readable matrices, which may or may not appear visually similar in size. The multiple matrices, though physically separate, may contain check values and features which assure the detection of any attempted alteration of either the human-readable text and/or the machine-readable matrices. In this regard, the encoded biometric data and textual data can be concatenated into one data string, divided by approximately two, and then formed into two matrices of approximately equal size.

[0027] Alternatively, the biometric data and text data may be interleaved, for example, in alternating bits, bytes, group of bytes, etc. to form a data string which is then divided into the two matrices. Preferably, each matrix is provided with a checksum for verifying the data integrity of each matrix independently. In addition, or alternatively, the matrices may have an interdependent checksum that is used to verify the data integrity of both matrices collectively. As a result of these checksums, if one matrix is altered, or if both matrices are altered, invalid data will be read. Advantageously, interleaving biometric data and textual data according to a predetermined routine enhances the ability to detect altered matrices.

[0028] Alternatively, biometric data set 101 could be formed as one matrix and textual data set 102 could be formed as a second matrix.

[0029] Enhanced data security is obtained and maintained by verifying the machine-readable data set for acceptability against predetermined criteria which may include searching a data base (e.g., an organized, comprehensive collection of data stored for use by processing system(s)) of previously issued articles to determine uniqueness. Note, in an alternate embodiment input data set 100 may be received at a remote access encodation site not equipped with the verification and/or encodation algorithm(s), in which case, a data signal representation or both the recipient-specific biometric data and the related textual data may be transmitted to a secure central host (shown in a similar context in FIG. 2A), the central host then performs the above mentioned verification. The transmission may be by wired or non-wired communication.

[0030] If the recipient is determined acceptable, the recipient-specific biometric data is encoded, which preferably includes utilization of compression algorithms, combining the biometric data subsets, and optionally, the textual data subsets, into one or more machine-readable matrices. If input data set 100 was received at a remote access encodation

site not equipped with the encodation algorithm(s), the resulting encoded binary string is transmitted as previously discussed to the remote access encodation site. A standard article issuance device (shown in FIG. 1B) then fixes the machine-readable data set onto one or more self-verifying articles. As the articles are created and ejected from the article issuance device, a record of the event is automatically entered into the data base, which, if input data set 100 is received at a remote access encodation site, may be located at the central host. Entry of the record insures that duplicate articles are not inadvertently issued at a later date. Note that the number of articles issued is directly related to the intended use of the articles.

[0031] Applications of this aspect of the invention include issuing only a single driver's license having a unique encoded photo, or issuing multiple articles, such as checks, traveler's checks, bank account withdrawal slips, etc. having the same encrypted signatures.

[0032] FIG. 1B illustrates an isometric view of processing system 103. Processing system 103 includes a personal computer ("PC") 105 coupled with a article issuance device 114. PC 105 is comprised of a hardware casing 106 (shown as having a cut away view), a monitor 109. a keyboard 110 and optionally a mouse 113.

[0033] Hardware casing 106 includes both a floppy disk drive 107 and a hard disk drive 108. Floppy disk drive 107 is operable to receive, read and write to external disks, while hard disk drive 108 is operable to provide fast access data storage and retrieval. Although only floppy disk drive 107 is illustrated, PC 105 may be equipped with any suitably arranged structure for receiving and transmitting data, including, for example, tape and compact disc drives, and serial and parallel data ports. Within the cut away portion of hardware casing 106 is a processing unit, central processing unit ("CPU") 111, coupled with a memory storage device, which in the illustrated embodiment is a random access memory ("RAM") 112. Although PC 105 is shown having a single CPU 111, PC 105 may be equipped with a plurality CPUs 111 operable to cooperatively carry out the principles of the present invention. Article generating device 114 is operable to receive one or more output data sets from PC 105, and fix the output data sets to the article's surface.

[0034] Although PC 105 and article generating device 114 have been utilized for illustrating one implementation of processing system 103, the invention may alternately be implemented within any processing system having at least one processing unit, including, for example, sophisticated calculators and hand held, mini, main frame and super computers, including RISC and parallel processing architectures, as well as within network combinations of the foregoing, and may utilize any suitably arranged article producing means.

[0035] FIG. 1C illustrates a conceptual block diagram of one of any number of sub-processing systems which may be utilized in conjunction with FIGS. 1A and 1B. The sub-processing system includes a single processing unit, such as CPU 111, coupled via data bus 118 with a memory storage device, such as RAM 112.

[0036] Memory storage device 112 is operable to store one or more instructions which processing unit 111 is operable to retrieve, interpret and execute. Processing unit 111 includes a control unit 115, an arithmetic logic unit ("ALU") 116, and a local memory storage device 117, such as, for example, stackable cache or a plurality of registers. Control unit 115 is operable to fetch instructions from memory storage device 112. ALU 116 is operable to perform a plurality of operations, including addition and Boolean AND needed to carry out instructions. Local memory storage device 117 is operable to provide high speed storage used for storing temporary results and control information.

[0037] FIG. 2A illustrates a functional block diagram of a system for verifying the authenticity of a received self-verifying article in accordance with the present invention. The system includes self-verifying article 104, a remote access site processing system 200, optionally coupled with a central host processing system 103 (as indicated by the broken line), and an authenticity message displaying means 201, such as a display device, a printer, or other suitably arranged indicating device.

[0038] Self-verifying article 104 includes at least one encoded data set which includes a first data subset that is an encoded copy of a portion, or the whole, of a biometric data set.

[0039] Self-verifying article 104 also includes both a text data set and a biometric data set.

[0040] Remote access site processing system 200 includes input means, processing means and output means. The input means are for receiving self-verifying article 104. The processing means are for verifying the authenticity of self-verifying article 104, which may include communications between remote access site processing system 200 and central host processing system 103.

[0041] The output means are for transmitting an authenticity message produced by the processing means to display means 201.

[0042] The processing means are operable to scan self-verifying article 104 to locate and decode the encoded first data set and to compare the decoded first data set with a second data set, which is either obtained from the bearer of the article or is fixed to self-verifying article 104, and to generate the output signal indicating authenticity of article 104. In an alternate embodiment, the processing means either selectively bypasses or is not operable to perform the comparison of the decoded first data set and the second data set. Instead, the processing means generates an output signal representative of the decoded first data set, e.g., a graphic image display of the portion of the biometric data set, and the second data set to a display device for manual comparison and verification by a processing system operator. Alternatively, the processing system operator may manually compare the decoded first data set, and optionally the

second data set (if one is fixed to the article), with the article bearer or a biometric data set obtained from the bearer, e.g., the bearer's signature or appearance, or from a database.

[0043] The illustrated system for verifying the authenticity of self-verifying article 104 may utilize a variety of devices including, for example, portable terminals, fixed station readers, and flat bed scanners, each of which may directly incorporate decoder capability or have decoder capability available at a base/host station, such as processing system 103, via wired or radio frequency, short wave, cellular, infrared or other form of non-wired communication. Remote access site processing system 200 and/or central host processing system 103 may be configured with keyboards and display screens of sufficient resolution to accurately display the encoded biometric image and/or textual data, and may incorporate imaging apparatus necessary to convert machine-readable data sets into binary machine language bits in preparation for decoding.The imaging apparatus may be based on any of a number of technologies, including CCD, CMOS, and NMOS or other forms of light sensitive sensors, which sensors may be structured in the form of a two dimensional area or one-dimensional linear arrays, or a single beam laser reading for scanning a two-dimensional image in a raster pattern.

[0044] One preferred embodiment of imaging apparatus is a linear array scanner that is vertically aligned with a solid border of an imprinted machine readable code 205, and when two or more matrices are used, these matrices are arrayed in parallel orientation so that the two symbols can be passed by the CCD scanner using a conventional card swipe action as in conventional magnetic strip reading. The matrices are then read and a video image of each matrix is stored in memory for processing. Imaging may also be achieved through the use of lasers, laser-diodes, infrared or other such binary imaging technologies which devices may also be structured in the form of two-dimensional area or one-dimensional linear arrays. Additionally, readers may include the ability to automatically verify the images and information encoded within the machine-readable matrix to the human recognizable version on the same article. In one embodiment, this comparison may be accomplished internal to remote access site processing system 200's memory thereby precluding the need for key pads and/or high resolution display screens on the terminals. Alternately, as introduced, operators may visually compare the information displayed on the terminal screen to the human readable information now present on the article and/or to the article bearer.

[0045] FIG. 2B illustrates an isometric view of a hand held computer which may be used as remote access site processing system 200. Hand held computer 200 includes a keypad 202, a display screen 203 and an input port 204. Keypad 202 includes a systematic arrangement of keys for manually receiving input data from a user. Display screen 203 is for displaying an authenticity message, and/or biometric and/or textual data.

[0046] Input port 204 is for receiving self-verifying article 104, here illustrated as a driver's license, which in the illustrated embodiment includes encrypted machine-readable data sets 205 a;b configured as two optically readable binary matrices. Remote access site processing system 200 includes at least one processing unit and one memory storage device, such as the subprocessing system illustrated in FIG. 1C. Preferably, the processing unit includes a microprocessor having associated memory (non-volatile storage for containing the program instruction set to identify and decode the matrices, and volatile memory for a data processing work area), a video memory for storing an image of the matrices to be decoded, and associated signal conditioning circuits, which are mounted on a single printed circuit board.

[0047] FIG. 3 illustrates a preferred single machine-readable binary coded matrix, generally indicated as a matrix 205. Matrix 205 is a sample of the Data Matrix symbology developed by
International Data Matrix, Inc., Clearwater, Florida, the assignee of this invention. Matrix 205 has a perimeter 300 formed by intersecting sides 301 formed of solid lines and intersecting perimeter sides 302 formed of dark perimeter squares 303 and light perimeter squares 304 in an alternating pattern.

[0048] Data, generally indicated as 305, is stored within perimeter 301 of matrix 204 by converting each character to be stored to a visual binary code represented by dark and light squares corresponding to ones and zeros of encoded binary information.

[0049] For a more complete description of the configuration of matrix 205, reference is made to United States Patent No. 4,939,354, entitled "Dynamically Variable Machine Readable Binary Code and
Method for Reading and Producing Thereof" and to co-pending patent application, United States patent 5,324,923, entitled "Apparatus for Producing a Dynamically Variable Machine Readable
Binary Code and Method for Reading and Producing Thereof," commonly owned by the assignee of this patent document.

[0050] FIG. 4A illustrates a flow diagram for producing an unalterable self-verifying article in accordance with the embodiment illustrated in FIG. 1A. Upon entering START block 400, the process according to the principles of the present invention begins. The recipient-specific data set, which is comprised of at least one data subset, is received by processing system 103 (input block 401). Processing system 103 preferably performs a graphic image compression of a first data subset.

[0051] Image compression by a factor of approximately 50:1 or better is preferred to obtain a digital representation of the acquired data. Such compressed data is capable of reproducing on a conventional graphic display screen the recipient specific image without any significant degradation of visual quality (block 402). The image compression may be by any standard routine e.g.,

Discrete Cosine Transform (DCT), LZW (Lempcl-Ziv), fractal, or others to reduce the amount of bits required to encode the first data subset. A compression ratio of 50:1 is deemed suitable, but other ratios may be used. In addition to data compression, a graphic image enhancement routine may be performed on the first data subset, preferably before the data compression step, in order to enhance the image contrast, sharpen and smooth edges and reduce the effect of shadows, particularly for imaging a photograph of the recipient. The foregoing improves the digital image for more effective data compression. Suitable image enhancement routines are known, and described R. Gonzalez et al., Digital Image Processing, published by Addison-Wesley Publishing Co. (Reading MA) 1987. Processing system 103 selectively encodes the compressed first data set, thereby generating a machine readable data set (processing block 403). This selectively encoding step is more fully discussed in connection with the detail description of FIG. 4B. Processing system 103 is further operable to configure the machine-readable data set as an optically readable binary code forming one or more matrices (processing block 404).

[0052] Processing system 103 fixes the machine-readable data set and the first recipient-specific data subset onto a surface of an article, thereby producing self-verifying article 104 (processing block 405). In one embodiment, the matrix is fixed on the article using a conventional printing process, e.g., thermal, thermal transfer, ink-jet, bubble-jet, laser jet, dot matrix printing, etc. Alternatively, the matrix or matrices may be fixed sub-surface, e.g., by laminating a top surface or by placing the matrix over the printed layer of a multilayer article. In another embodiment, the machine-readable data set is imprinted over an already printed area of the article, such as the photograph on a driver's license for example. In yet another embodiment, the matrix is formed by introducing bubbles or voids into the article, or drilling or punching holes into or through the article, according to the matrix pattern, such that the code is machine readable by a technique capable of detecting the absence or presence of material, or the relative density of material, or the depth of a bubble, void, hole or the like in the article, e.g., ultrasonically, or by a light measuring system or other suitable imaging system having a bounceback signal capable of distinguishing the code.

[0053] FIG. 4B illustrates a more detailed flow diagram of processing block 402 illustrated in FIG. 4A. Upon entering START block 406, the selective encodation of the first data set begins.

[0054] Processing system 103 compares the first data set with system control values to determine if the first data set is within acceptable tolerances (processing block 407). The step of comparing may include, for example, syntactic and/or semantic analysis. If it is determined that the first data set is invalid as received ("N" branch of decisional block 408), then processing system 103 aborts self-verifying article production (termination block 409). Alternatively, if it is determined that the first data set is valid as received ("Y" branch of decisional block 408), then processing system 103 searches a data base of previously issued articles to determine if the issued article is unique (processing block 410), uniqueness being determined on a subjective basis as a function of the type of article being produced. Note that the data base utilized by processing system 103 may be internal or external to processing system 103, and that in either system, processing system 103 may search the data base directly, or indirectly. For example, the data base may be stored remotely and controlled by another processing system with which processing system 103 communicates. If it is determined that the first data set is not unique as received ("N" branch of decisional block 411), then processing system 103 aborts self verifying article production (termination block 412).

[0055] Alternatively, if it is determined that the first data set is valid as received ("Y" branch of decisional block 411), then processing system 103 selectively inserts one or more subsets of the received recipient-specific data set as al least one record into the data base (processing block 413). Processing system 103 then encodes the first data set (processing block 414), and in one embodiment adds error correction bits to the encoded first data set (processing block 415).

[0056] The selective encodation of only the first data set as embodied within FIGS. 4A and 4B was for illustrative purposes only, and it is understood that among the various aspects and features of the present invention is the ability to selectively encode a plurality of compressed recipient-specific data subsets, and to subsequently concatenate, interleave, etc. the encoded subsets, thereby forming a single machine-readable data set.

[0057] Further, when two or more data subsets are encoded and concatenated, interleaved, etc. together, processing system 103 is operable to configure the machine-readable data set into one or more optically readable matrices wherein individual encoded data subsets may span two or more matrices.

[0058] FIG. 5 illustrates a flow diagram for verifying the authenticity of a received self-verifying article in accordance with the embodiment illustrated in FIG. 2A. Upon entering START block 500, the process according to the principles of the present invention begins. The self-verifying article, which in this embodiment includes a plurality of data sets wherein a first data set is an encoded copy of a second data set, is received by a remote access site processing system 200 (input block 501).

[0059] Remote access site processing system 200 then scans the received self-verifying article to locate the encoded first data set (processing block 502). Remote access site processing system 200 decodes the encoded first data set (processing block 503), and compares the decoded first data set with the second data set to determine the authenticity ot the received self-verifying article (processing block 504).

[0060] The comparison step is accomplished through communications between remote access site processing system 200 and processing system 103, wherein processing system 103 maintains a data base of recipient-specific data relating

to previously issued self-verifying articles. Communications between remote access site processing system 200 and processing system 103 may be accomplished via wired or nonwired communication means. In an alternate embodiment, at least the decoded first data set, and optionally the second data set, are transmitted to an output display device for manual comparison by a system operator. If it is determined that the decoded first data set is not authentic ("N" branch of decisional block 505), then remote access site processing system 200 displays an authenticity message 201 indicating that the self-verifying article is invalid (output block 506). Alternatively, if it is determined that the decoded first data set is authentic ("Y" branch of decisional block 505), then remote access site processing system 200 displays an authenticity message 201 indicating that the self-verifying article is valid (output block 507).

[0061] In another embodiment, prior to decoding the encoded first data set, remote access site processing system 200 converts the received self-verifying article into a digital bit-map image, and separates the digital bit-map image into a plurality of regions, wherein a first region includes the encoded first data set and a second region includes the second data set. In this embodiment, both the first and second regions may include a plurality of biometric and/or textual data subsets which remote site processing system 200 is further operable to convert into common data formats for processing.

[0062] As noted previously, one embodiment of the self verifying article contains two matrices which have a first data set of biometric data and a second data set of textual data. In addition, in one embodiment, the article also may contain a magnetic stripe for containing alterable data, which may be programmed by scanning the machine readable matrices, decoding certain data contained therein and, decoding that data (with or without other data), onto the magnetic stripe. This makes the self verifying article useful in applications which require reading a magnetic stripe.

[0063] A further use of the invention is to prevent software piracy. Software is a special form of program which has been recorded to a storage medium, such as one of the above identified storage mediums. Software enables programs to be freely transferred or copied from one storage medium to another, which enables unlicensed users to obtain illegal copies of the software. For example, in one embodiment, the purchaser of a processing system provides a hardware vendor with industry standardized personal data, which may include biometric data, which is, optionally encrypted, and stored internal to the processing system. Whenever the processing system purchaser buys software, the purchaser is again required to provide such industry standardized personal data, which is compressed, optionally encrypted, encoded into a machine-readable data set, preferably as one or more binary coded matrices, and fixed to the surface of a portable storage medium, such as a floppy or compact disk. When the software is loaded onto the processing system, the matrices are scanned, decoded and verified in accordance with the principles of the present invention, compared with the previously stored data to ensure a commonality of ownership, thereby limiting software piracy. If common ownership is found, then the software is loaded onto the processing system along with the decoded industry standardized personal data. In the event the processing system owner transfers ownership of the processing system, the new owner, in order to load his software, will have to have the industry standardized personal data redefined, which could suspend the new owner's use of the existing software or automatically delete the existing software. In the event use of the software is suspended, a "transfer" of ownership routine might be available to reactivate the suspended use of the existing software if ownership of the particular software was legally transferred.

[0064] Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the scope of the appended claims.

Claims

1. A method for producing a recipient-specific self-verifying article, said method comprising the steps of: receiving a recipient-specific biometric data set, said recipient-specific data set comprised of one or more recipient specific data subsets; encoding a first recipient-specific biometric data subset to generate a machine readable data set; configuring said machine readable data set as an optically readable binary code forming at least one matrix (205); and fixing, said machine-readable data set to an article, **characterised in that** said comparing step, upon a determination of acceptability, further includes the step of: searching a database of previously produced unalterable articles to determine if said recipient-specific biometric data set is unique, said database of previously produced unalterable articles comprising one or more records; upon a determination of non-uniqueness aborting production of said unique recipient-specific identification article; and upon a determination of uniqueness inserting said recipient-specific biometric data set into at least one of said records within said database of previously produced unalterable articles.

2. The method as set forth in Claim 1 wherein said encoding step further includes the step of: comparing at least a portion of said first recipient-specific biometric data subset with a control value to determine if said first recipient-specific data subset is within acceptable tolerance of said control value.

3. The method as set forth in any preceding claim wherein said configuring step is preceded by the steps of: selectively

encoding a second recipient data subset.

4. The method as set forth in Claim 1 or 2 wherein said configuring step is preceded by the steps of: selectively encoding a second recipient data subset; and combining said encoded second recipient-specific data subset with said encoded first recipient-specific data subset thereby forming said machine-readable data set.

5. The method as set forth in any preceding claim wherein said fixing step further includes the step of etching said matrix (205) into said article.

6. The method as set forth in any preceding claim wherein said fixing step further includes the step of indenting said matrix (205) in said article.

7. The method as set forth in any preceding claim wherein said encoding step further includes the step of encrypting said first recipient-specific biometric data subset.

8. The method as set forth in Claim 7 when dependent on claim 4 or 5
wherein said combining step includes the step of: interleaving said encoded second recipient-specific data subset with said encoded first recipient specific biometric data subset.

9. The method as set forth in any preceding claim when dependent on claim 3 or 4 wherein said second recipient-specific data subset includes textual data (102).

10. The method as set forth in Claim 1 wherein said encoding step further includes the step of: configuring said machine readable data set as an optically readable binary code forming two matrices.

11. A method for verifying the authenticity of a received recipient-specific self-verifying article, said recipient-specific self-verifying article including a plurality of data sets including a first biometric data set and a second biometric data set wherein said first data set is an encoded copy of said second data set, said method comprising the steps of: scanning said received recipient-specific article to locate said encoded first biometric data set; decoding said encoded first biometric data set; and comparing said decoded first biometric data set with said second biometric data set to determine the authenticity of said received recipient-specific identification article, **characterised in that** the plurality of data sets includes textual data, the first biometric data set being interleaved with an encoded copy of the textual data according to a predetermined routine and configured as a matrix of optically machine readable binary data, the matrix being provided with a check sum and wherein the method includes the step of detecting whether the matrix has been altered by reading the matrix in light of the check sum and checking whether invalid data is read.

12. The method as set forth in Claim 11 wherein said scanning step further includes the step: converting said plurality of data sets into a digital bit-map image; and separating said digital bit-map image into a plurality of regions,
wherein a first region includes said encoded first data set and a second region includes said second data set.

13. The method as set forth in Claim 12 wherein said first region includes an encoded textual data subset (102) and said decoding step further includes the step of: converting said first region decoded textual data subset (102) and a second region textual data subset (102) to a first data format.

14. The method as set forth in Claim 12 wherein said first region includes an encoded biometric data subset (101) and said decoding step further includes the step of: converting said first region decoded biometric data subset (101) and a second region biometric data subset (101) to a first data format.

15. The method as set forth in Claim II wherein said comparing step further includes the step of: transmitting said decoded first data set and said second data to a processing system for said determination of authenticity.

16. A processing system for producing a unique machine-readable data set for fixing upon a self-authenticating recipient-specific article, said processing system comprising: an input port operable to receive a recipient-specific biometric data set, said recipient-specific biometric data set comprised of at least one recipient-specific biometric data subset; a memory storage device operable to store a plurality of processing system instructions; a processing unit for generating said machine-readable data set for imprinting upon a self-authenticating recipient-specific article by retrieving and executing at least one of said processing unit instructions from said memory storage device, said processing unit operable to encode a first recipient-specific biometric data subset; and an output port for transmitting

said encoded first recipient-specific biometric data subset as said machine-readable data set;
wherein said processing unit is further operable to configure said encoded first recipient-specific biometric data subset as an optically readable binary code forming at least one matrix (205) **characterised in that** the system further comprises: means for searching a database of previously produced self-authenticating articles to determine if said recipient-specific data set is unique, said database of previously produced self-authenticating articles comprised of one or more records; and means for inserting said recipient-specific data set into at least one of said records within said database of previously produced self-authenticating articles upon a determination of uniqueness.

17. The processing system as set forth in Claim 16 wherein said processing unit is further operable to: selectively encode a second recipient-specific data subset; and combine said encoded second recipient-specific data subset with said encoded first recipient-specific data subset thereby forming said machine-readable data set.

18. The processing system as set forth in Claim 17 wherein said processing unit is further operable to configure said machine readable data set as an optically readable binary code forming two matrices.

19. The processing system as set forth in Claim 16 further comprising: means for comparing said first recipient-specific data subset with one or more control values to determine if said first recipient-specific data subset is valid.

20. The processing system as set forth in Claim 16 further comprising: an article production device, coupled with said output port, for fixing said machine-readable data set on a self-authenticating recipient-specific article.

21. The processing system as set forth in Claim 20 wherein said article production device further comprise means for fixing at least a portion of the recipient-specific data set on said self-authenticating article.

22. A processing system for verifying the authenticity of a self-verifying article (104), said processing system comprising: an input port operable to receive a biometric data set including first and second data subsets wherein said first data subset is an encoded version of a second data subset, said input port including means controlled by a processing unit for selectively scanning the surface of said self-verifying article (104); a memory storage device operable to store a plurality of processing system instructions; said processing unit for verifying the authenticity of said self-verifying article (104) by retrieving and executing at least one of said processing unit instructions from said memory storage device, said processing unit operable to decode said encoded first data subset, **characterised in that** the input port is operable to receive textual data, wherein the first biometric data set is interleaved with an encoded copy of the textual data and configured as a matrix of optically machine readable binary data, the matrix being provided with a check sum and wherein the system is operable to detect whether the matrix has been altered by reading the matrix in light of the check sum and checking whether invalid data is read

23. The processing system as set forth in Claim 22 further comprising means for comparing said decoded first data subset with said second data subset.

24. The processing unit as set forth in Claim 23 further comprising means for generating an output signal indicating the authenticity of said self-verifying article (104).

25. The processing, system as set forth in Claim 22 wherein said processing unit is further operable to: convert said received data set to a digital bit-map image; and selectively separate said digital bit-map image into a plurality of regions, wherein a first region includes said encoded first data subset and a second region includes said second data subset.

26. The processing system as set forth in Claim 25 wherein said first region and said second region each include a biometric data subset (101) and said processing unit is further operable to convert said first region biometric data subset (101) and said second region biometric data subset (101) to a first data format.

27. The processing system as set forth in Claim 24 wherein said first region and said second region each include a textual data subset (102) and said processing unit is further operable to convert said first region textual data subset (102) and said second region textual data subset (102) to a first data format.

28. The processing system as set forth in Claim 22 further comprising means for displaying said decoded first data subset.

Patentansprüche

1. Verfahren zur Erzeugung eines Empfänger-spezifischen selbstüberprüfenden Artikels, wobei das Verfahren die Schritte umfasst: Empfangen eines Empfänger-spezifischen biometrischen Datensatzes, wobei der Empfänger-spezifische Datensatz einen oder mehrere Empfänger-spezifische Unter-Datensätze umfasst; Kodierung eines ersten Empfänger-spezifischen biometrischen Unter-Datensatzes zur Erzeugung eines Maschinen-lesbaren Datensatzes; Konfigurieren des Maschinen-lesbaren Datensatzes in einen optisch lesbaren Binärcode in Form mindestens einer Matrix (205); und Anbringen des Maschinen-lesbaren Datensatzes an einem Artikel, **dadurch gekennzeichnet, dass** der erwähnte Vergleichsschritt während der Feststellung der Annahmefähigkeit weiterhin den folgenden Schritt einschließt: Durchsuchen einer Datenbasis von früher erzeugten unabänderbaren Artikeln, um festzustellen ob der Empfänger-spezifische biometrische Datensatz einzigartig ist, wobei die Datenbasis von früher erzeugten Artikeln eine oder mehrere Protokolle umfasst; bei Feststellung der Nicht-Einzigartigkeit Verwerfen der Erzeugung das einzigartigen Empfänger-spezifischen Artikels; und bei Feststellung der Einzigartigkeit Einfügen des Empfänger-spezifischen biometrischen Datensatzes in mindestens eines der Protokolle innerhalb der Datenbasis von früher erzeugten unabänderbaren Artikeln.

2. Verfahren nach Anspruch 1, wobei der Kodierungsschritt weiterhin umfasst den Schritt: Vergleich mindestens eines Teils des ersten Empfänger-spezifischen biometrischen Unter-Datensatzes mit einem Kontrollwert, um festzustellen, ob der ersten Empfänger-spezifische Unter-Datensatz innerhalb akzeptierbarer Toleranzen des Kontrollwertes ist.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei dem Konfigurationsschritt vorausgeht der Schritt: selektive Kodierung eines zweiten Empfänger-Unterdatensatzes.

4. Verfahren nach Anspruch 1 oder 2, wobei dem Konfigurationsschritt vorausgeht der Schritt: selektive Kodierung eines zweiten Empfänger-spezifische Unterdatensatzes; und Zusammenführen des verschlüsselten zweiten Empfänger-spezifischen Unter-Datensatzes mit dem verschlüsselten ersten Empfänger-spezifischen Unter-Datensatzes, wodurch der Maschinen-lesbare Datensatz gebildet wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Anbringungsschritt den Schritt des Ätzens der Matrix (205) in den Artikel einschließt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Anbringungsschritt den Schritt des Einkerbens der Matrix (205) in den Artikel einschließt.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Kodierungsschritt weiterhin die Verschlüsselung des ersten Empfänger-spezifischen biometrischen Unter-Datensatzes umfasst.

8. Verfahren nach Anspruch 7 soweit abhängig von Anspruch 4 oder 5, wobei der Zusammenführungsschritt umfasst den Schritt: Durchschießen des kodierten zweiten Empfänger-spezifischen Unter-Datensatzes mit dem kodierten ersten Empfänger-spezifischen biometrischen Unter-Datensatzes.

9. Verfahren nach einem der vorhergehenden Ansprüche soweit abhängig von Anspruch 3 oder 4, wobei der zweite Empfänger-spezifische Unter-Datensatz textliche Daten (102) umfasst.

10. Verfahren nach Anspruch 1, wobei der Kodierungsschritt einschließt den Schritt: Konfigurieren des Maschinen-lesbaren Datensatzes in einen optisch lesbaren, zwei Matrizen bildenden Binärcode.

11. Verfahren zur Verifizierung die Authentizität eines entgegengenommenen Empfänger-spezifischen selbstverifizierenden Artikels, wobei der Empfänger-spezifische selbstverifizierende Artikel eine Vielzahl von Datensätzen einschließlich einen ersten biometrischen Datensatz und einen zweiten biometrischen Datensatz umfasst, wobei der erste Datensatz eine kodierte Kopie des zweiten Datensatzes ist, umfassend folgende Schritte: Scannen des entgegengenommenen Empfänger-spezifischen Artikels zur Ortung des kodierten ersten biometrischen Datensatzes; Dekodieren des kodierten ersten biometrischen Datensatzes; und Vergleichen des dekodierten ersten biometrischen Datensatzes mit dem zweiten biometrischen Datensatz um die Authentizität des entgegengenommenen Empfänger-spezifischen Identifizierungs-Artikels festzustellen, **dadurch gekennzeichnet, dass** die Vielzahl von Datensätzen textliche Daten umfasst, der erste biometrische Datensatz mit einer kodierten Kopie des textlichen Datensatzes entsprechend einer vorbestimmten Routine durchschossen ist und als eine Matrix von optisch Maschinen-lesbaren binären Daten konfiguriert ist, wobei die Matrix mit einer Prüf-Summe versehen ist, und wobei das Verfahren den

Schritt der Feststellung umfasst, ob die Matrix geändert wurde, indem die Matrix im Lichte der Prüf-Summe gelesen wird und Prüfen, ob ungültige Daten gelesen werden.

12. Verfahren nach Anspruch 11, wobei der Scan-Schritt weiterhin umfasst den Schritt: Umwandlung der Datensatze in ein digitales Bit-Map-Bild; und Aufteilung des Bit-Map-Bildes in eine Vielzahl von Regionen, wobei eine erste Region den ersten kodierten Datensatz umfasst und eine zweite Region den zweiten Datensatz umfasst.

13. Verfahren nach Anspruch 12, wobei die erste Region einen kodierten textlichen Unter-Datensatz (102) umfasst und der Dekodierschritt weiterhin umfasst den Schritt: Umwandlung des dekodierten textlichen Unter-Datensatzes (102) der ersten Region und eines textlichen Unterdatensatzes der zweiten Region in ein erstes Datenformat.

14. Verfahren nach Anspruch 12, wobei die erste Region einen kodierten biometrischen Unter-Datensatz (101) umfasst und der Dekodierschritt weiterhin umfasst den Schritt: Umwandlung des dekodierten biometrischen Unter-Datensatzes (101) der ersten Region und eines zweiten biometrischen Unter-Datensatzes (101) in ein erstes Datenformat.

15. Verfahren nach Anspruch 11, wobei der Vergleichsschritt weiterhin umfasst den Schritt: Übermittlung des ersten Datensatzes und des zweiten Datensatzes zu einem Verarbeitungssystem zur Bestimmung der Authentizität.

16. Verarbeitungssystem zur Erzeugung eines einzigartigen Maschinen-lesbaren Datensatzes zur Anbringung an einem selbst authentifizierendem Empfänger-spezifischen Artikel, wobei das Verarbeitungssystem umfasst: eine Eingabe-Pforte bedienbar zur Aufnahme eines Empfänger-spezifischen biometrischen Datensatzes, wobei der Empfänger-spezifische biometrische Datensatz mindestens einen Empfänger-spezifischen biometrischen Unter-Datensatz umfasst; eine Speichereinheit bedienbar zur Speicherung einer Vielzahl von Verarbeitungssystem-Anweisungen; eine Verarbeitungseinheit zur Erzeugung des Maschinen-lesbaren Datensatzes zur Einprägung auf einem selbst authentifizierenden Empfänger-spezifischen Artikel durch Aufrufen und Ausführung mindestens einer der Anweisungen des Verarbeitungssystems von der Speichereinheit, wobei die Verarbeitungseinheit bedienbar ist zur Kodierung eines ersten Empfänger-spezifischen biometrischen Unter-Datensatzes; und eine Ausgabe-Pforte zur Übermittelung des kodierten ersten Empfänger-spezifischen biometrischen Unter-Datensatzes als Maschinen-lesbarer Datensatz; wobei die Verarbeitungseinheit weiterhin bedienbar ist zur Konfiguration des kodierten ersten Empfänger-spezifischen biometrischen Unter-Datensatzes in einen optisch lesbaren Binärcode in Form mindestens einer Matrix (205), **dadurch gekennzeichnet, dass** das System weiterhin umfasst: Mittel zur Durchsuchung einer Datenbasis von früher erzeugten selbst authentifizierenden Artikeln, um festzustellen, ob der Empfänger-spezifische Datensatz einzigartig ist, wobei die Datenbasis von früher erzeugten selbst authentifizierenden Artikeln ein oder mehrere Protokolle umfasst; und Mittel zur Einfügung des Empfänger-spezifischen Datensatzes in mindestens eines der Protokolle innerhalb der Datenbasis von früher erzeugten selbst authentifizierenden Artikeln bei Feststellung der Einzigartigkeit.

17. Verarbeitungssystem nach Anspruch 16, wobei die Verarbeitungseinheit ferner bedienbar ist, um: einen zweiten Empfänger-spezifischen Unter-Datensatz selektiv zu kodieren; und den zweiten Empfänger-spezifischen Unter-Datensatz mit dem kodierten ersten Empfänger-spezifischen Unter-Datensatz zu verbinden, wobei der Maschinen-lesbare Datensatz gebildet wird.

18. Verarbeitungssystem nach Anspruch 17, wobei die Verarbeitungseinheit ferner bedienbar ist, um den Maschinen-lesbaren Datensatz in einen optisch lesbaren, zwei Matrizen bildenden Binärcode zu konfigurieren.

19. Verarbeitungssystem nach Anspruch 16, weiterhin umfassend:

Mittel zum Vergleichen das ersten Empfänger-spezifischen Unter-Datensatzes mit einem oder mehreren Kontrollwerten, um festzustellen, ob der erste Empfänger-spezifische Unter-Datensatz gültig ist.

20. Verarbeitungssystem nach Anspruch 16, weiterhin umfassend:

eine Vorrichtung zur Erzeugung des Artikels, die mit der Ausgabe-Pforte verbunden ist, um den Maschinen-lesbaren Datensatz auf einem selbst authentifizierenden Empfänger-spezifischen Artikel zu fixieren.

21. Verarbeitungssystem nach Anspruch 20, wobei die Vorrichtung zur Erzeugung des Artikels weiterhin Mittel umfasst, um mindestens einen Teil des Empfänger-spezifischen Datensatzes auf dem selbst authentifizierenden Artikel zu fixieren.

22. Verarbeitungssystem zur Verifizierung der Authentizität eines selbst verifizierenden Artikels (104), umfassend: eine Eingabe-Pforte bedienbar um einen biometrischen Datensatz, umfassend erste und zweite Unter-Datensätze, zu empfangen, wobei der erste Unter-Datensatz eine kodierte Version eines zweiten Unter-Datensatzes ist, wobei die Eingabe-Pforte von einer Verarbeitungseinheit gesteuerte Mittel enthält, um die Oberfläche des selbst verifizierenden Artikels (104) selektiv zu scannen; eine Speichereinheit bedienbar, um eine Vielzahl von Anweisungen an das Verarbeitungssystem zu speichern; die Verarbeitungseinheit zur Verifizierung der Authentizität des selbst verifizierenden Artikels (104) durch Rückgriff auf und Ausführung mindestens einer der Anweisungen an die Verarbeitungseinheit aus der Speichereinheit, wobei die Verarbeitungseinheit bedienbar ist, um den kodierten ersten Unter-Datensatz zu dekodieren, **dadurch gekennzeichnet, dass** die Eingabe-Pforte bedienbar ist, um textliche Daten zu empfangen, wobei der erste biometrische Datensatz mit einer kodierten Kopie der textlichen Daten durchschossen ist und als eine Matrix von optisch Maschinen-lesbaren binären Daten konfiguriert ist, die Matrix eine Prüfsumme aufweist und wobei das System bedienbar ist um festzustellen, ob die Matrix abgeändert wurde, indem die Matrix im Lichte der Prüfsumme gelesen wird und geprüft wird, ob ungültige Daten gelesen werden.

23. Verarbeitungssystem nach Anspruch 22, weiterhin enthaltend Mittel zum Vergleichen des dekodierten ersten Unter-Datensatzes mit dem zweiten Unter- Datensatz.

24. Verarbeitungseinheit nach Anspruch 23, weiterhin Mittel zur Erzeugung eines Ausgangssignals, das die Authentizität des selbst verifizierenden Artikels (104) anzeigt, aufweisend.

25. Verarbeitungssystem nach Anspruch 22, wobei die Verarbeitungseinheit weiterhin bedienbar ist um: den erhaltenen Datensatz in ein digitales Bit-Map-Bild umzuwandeln; und das digitale Bit-Map-Bild in eine Vielzahl von Regionen selektiv zu unterteilen, wobei eine erste Region den kodierten ersten Unter-Datensatz umfasst und eine zweite Region den zweiten Unter-Datensatz umfasst.

26. Verarbeitungssystem nach Anspruch 25, wobei die erste Region und die zweite Region jeweils einen biometrischen Unter-Datensatz (101) einschließen und die Verarbeitungseinheit ferner bedienbar ist, um den biometrischen Unter-Datensatz (101) der ersten Region und den biometrischen Unter-Datensatz (101) der zweiten Region in ein erstes Datenformat zu konvertieren.

27. Verarbeitungssystem nach Anspruch 24, wobei die erste Region und die zweite Region jeweils textliche Unter-Datensätze (102) umfassen und die Verarbeitungseinheit ferner bedienbar ist, um den ersten textlichen Unter-Datensatz der ersten Region und den zweiten textlichen zweiten Unter-Datensatz der zweiten Region in ein erstes Datenformat umzuwandeln.

28. Verarbeitungssystem nach Anspruch 22, weiterhin Mittel zur Darstellung des dekodierten ersten Unter-Datensatzes aufweisend.

Revendications

1. Procédé de production d'un article auto-vérificateur spécifique du bénéficiaire, le procédé comprenant les étapes suivantes :

la réception d'un ensemble de données biométriques spécifiques d'un bénéficiaire, l'ensemble de données spécifiques d'un bénéficiaire étant formé d'un ou plusieurs sous-ensembles de données spécifiques du bénéficiaire, le codage d'un premier sous-ensemble de données biométriques spécifiques du bénéficiaire pour la création d'un ensemble de données lisibles par la machine, la configuration de l'ensemble de données lisibles par la machine sous forme d'un code binaire lisible optiquement formant au moins une matrice (205), et la fixation de l'ensemble de données lisibles par la machine sur un article, **caractérisé en ce que** l'étape de comparaison, après détermination de l'acceptabilité, comporte en outre les étapes suivantes : la recherche d'une base de données d'articles inaltérables produits auparavant pour la détermination du fait que l'ensemble de données biométriques spécifiques du bénéficiaire est unique, la base de données d'articles inaltérables produits auparavant comprenant un ou plusieurs enregistrements, dans le cas de la détermination du défaut d'unicité, l'abandon de la production de l'article unique d'identification spécifique du bénéficiaire, et, après détermination de l'unicité, l'insertion de l'ensemble de données biométriques spécifiques du bénéficiaire dans l'un au moins des enregistrements dans la base de données des articles inaltérables produits auparavant.

2. Procédé selon la revendication 1, dans lequel l'étape de codage comprend en outre l'étape de comparaison d'une partie au moins du premier sous-ensemble de données biométriques spécifiques du bénéficiaire à une valeur de commande pour la détermination du fait que le premier sous-ensemble de données spécifiques du bénéficiaire se trouve dans une plage de tolérances acceptable de la valeur de commande.

3. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de configuration est précédée par l'étape de codage sélectif d'un second sous-ensemble de données du bénéficiaire.

4. Procédé selon la revendication 1 ou 2, dans lequel l'étape de configuration est précédée par des étapes de codage sélectif d'un second sous-ensemble de données de bénéficiaire, et de combinaison du second sous-ensemble codé de données spécifiques du bénéficiaire avec le premier sous-ensemble codé de données spécifiques du bénéficiaire avec ainsi formation de l'ensemble de données lisibles par la machine.

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de fixation comprend en outre l'étape de gravure de la matrice (205) dans l'article.

6. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de fixation comprend en outre l'étape d'entaille de la matrice (205) dans l'article.

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'étape de codage comprend en outre l'étape de chiffrage du premier sous-ensemble de données biométriques spécifiques du bénéficiaire.

8. Procédé selon la revendication 7 lorsqu'elle dépend de la revendication 4 ou 5, dans lequel l'étape de combinaison comprend une étape d'entrelacement du second sous-ensemble codé de données spécifiques du bénéficiaire avec le premier sous-ensemble codé de données biométriques spécifiques du bénéficiaire.

9. Procédé selon l'une quelconque des revendications précédentes lorsqu'elle dépend de la revendication 3 ou 4, dans lequel le second sous-ensemble de données spécifiques du bénéficiaire contient des données de texte (102).

10. Procédé selon la revendication 1, dans lequel l'étape de codage comprend en outre l'étape de configuration de l'ensemble de données lisibles par la machine sous forme d'un code binaire lisible optiquement formant deux matrices.

11. Procédé de vérification de l'authenticité d'un article auto-vérificateur spécifique du bénéficiaire et qui a été reçu, l'article auto-vérificateur spécifique du bénéficiaire comprenant plusieurs ensembles de données contenant un premier ensemble de données biométriques et un second ensemble de données biométriques, dans lequel le premier ensemble de données est une copie codée du second ensemble de données, le procédé comprenant les étapes suivantes : la lecture de l'article reçu spécifique du bénéficiaire pour la localisation du premier ensemble codé de données biométriques, le décodage du premier ensemble codé de données biométriques, et la comparaison du premier ensemble décodé de données biométriques au second ensemble de données biométriques pour la détermination de l'authenticité de l'article reçu d'identification spécifique du bénéficiaire, et étant **caractérisé en ce que** les ensembles de données comprennent des données de texte, le premier ensemble de données biométriques étant entrelacé avec une copie codée de données de texte en fonction d'un programme prédéterminé et ayant la configuration d'une matrice de données binaires lisibles optiquement par une machine, la matrice ayant une somme de vérification, et le procédé comprend l'étape de détection du fait que la matrice a été altérée par lecture de la matrice en fonction de la somme de vérification, et de vérification si des données invalides sont lues.

12. Procédé selon la revendication 11, dans lequel l'étape de lecture comprend en outre l'étape de conversion des ensembles de données en une image numérique en mode points, et de séparation de l'image numérique en mode points en plusieurs régions dans lesquelles une première région comprend le premier ensemble codé de données et une seconde région contient le second ensemble de données.

13. Procédé selon la revendication 12, dans lequel la première région contient un sous-ensemble codé de données de texte (102), et l'étape de décodage comprend en outre l'étape de conversion du sous-ensemble décodé de données de texte de la première région (102) et d'un sous-ensemble de données de texte d'une seconde région (102) à un premier format de données.

14. Procédé selon la revendication 12, dans lequel la première région comprend un sous-ensemble codé de données

biométriques (101) et l'étape de décodage comprend en outre l'étape de conversion du sous-ensemble de données biométriques décodées de la première région (101) et d'un sous-ensemble de données biométriques de la seconde région (101) à un premier format de données.

15. Procédé selon la revendication 11, dans lequel l'étape de comparaison comprend en outre l'étape de transmission du premier ensemble décodé de données et des secondes données à un système de traitement pour la détermination de l'authenticité.

16. Système de traitement destiné à produire un ensemble unique de données lisibles par la machine destiné à être fixé sur un article à authentification automatique et spécifique du bénéficiaire, le système de traitement comprenant une voie d'entrée destinée à fonctionner pour recevoir un ensemble de données biométriques spécifiques d'un bénéficiaire, l'ensemble de données biométriques spécifiques du bénéficiaire étant formé d'au moins un sous-ensemble de données biométriques spécifiques du bénéficiaire, un dispositif de mémorisation à mémoire destiné à mémoriser plusieurs instructions de système de traitement, une unité de traitement destinée à créer l'ensemble de données lisibles par la machine destinées à être imprimées sur un article à authentification automatique spécifique du bénéficiaire par récupération et exécution d'au moins l'une des instructions de l'unité de traitement dans le dispositif de mémorisation à mémoire, l'unité de traitement étant destinée à coder un premier sous-ensemble de données biométriques spécifiques du bénéficiaire, et une voie de sortie destinée à transmettre le premier sous-ensemble codé de données biométriques spécifiques du bénéficiaire sous forme d'un ensemble de données lisibles par la machine, dans lequel l'unité de traitement est en outre destinée à configurer le premier sous-ensemble codé de données biométriques spécifiques du bénéficiaire sous forme d'un code binaire lisible optiquement formant au moins une matrice (205),
caractérisé en ce que le système comporte en outre un dispositif destiné à chercher dans une base de données d'articles à authentification automatique produits auparavant pour la détermination du fait que l'ensemble de données spécifiques du bénéficiaire est unique, la base de données des articles à authentification automatique produits auparavant étant formée d'un ou plusieurs enregistrements, et un dispositif destiné à insérer l'ensemble de données spécifiques du bénéficiaire dans l'un au moins des enregistrements de la base de données d'articles à authentification automatique produits auparavant après détermination de l'unicité.

17. Système de traitement selon la revendication 16, dans lequel l'unité de traitement est en outre destinée à coder sélectivement un second sous-ensemble de données spécifiques du bénéficiaire, et à combiner le second sous-ensemble codé de données spécifiques du bénéficiaire avec le premier sous-ensemble codé de données spécifiques du bénéficiaire avec formation de cette manière de l'ensemble de donnés lisibles par la machine.

18. Système de traitement selon la revendication 17, dans lequel l'unité de traitement est en outre destinée à donner à l'ensemble de données lisibles par la machine une configuration d'un code binaire lisible optiquement formant deux matrices.

19. Système de traitement selon la revendication 16, comprenant en outre un dispositif de comparaison du premier sous-ensemble de données spécifiques du bénéficiaire à une ou plusieurs valeurs de commande pour la détermination du fait que le premier sous-ensemble de données spécifiques du bénéficiaire est valide.

20. Système de traitement selon la revendication 16, comprenant en outre un dispositif de production d'articles, couplé à la voie de sortie et destiné à fixer l'ensemble de données lisibles par la machine sur un article à authentification automatique spécifique du bénéficiaire.

21. Système de traitement selon la revendication 20, dans lequel le dispositif de production d'articles comprend en outre un dispositif destiné à fixer une partie au moins de l'ensemble de données spécifiques du bénéficiaire sur l'article à authentification automatique.

22. Système de traitement destiné à vérifier l'authenticité d'un article auto-vérificateur (104), le système de traitement comprenant une voie d'entrée destinée à recevoir un ensemble de données biométriques comprenant un premier et un second sous-ensemble de données tels que le premier sous-ensemble de données est une version codée d'un second sous-ensemble de données, la voie d'entrée comprenant un dispositif commandé par une unité de traitement et destiné à lire sélectivement la surface de l'article auto-vérificateur (104), un dispositif de mémorisation à mémoire destiné à mémoriser plusieurs instructions du système de traitement, l'unité de traitement étant destinée à vérifier l'authenticité de l'article auto-vérificateur (104) par récupération et exécution de l'une au moins des instructions d'unité de traitement depuis le dispositif de mémorisation à mémoire, l'unité de traitement étant destinée

à décoder le premier sous-ensemble codé de données, **caractérisé en ce que** la voie d'entrée est destinée à recevoir des données de texte, dans lesquelles le premier ensemble de données biométriques est entrelacé à une copie codée des données de texte et a une configuration de matrice de données binaires lisibles optiquement par la machine, la matrice ayant une somme de vérification, et le système est destiné à détecter le fait que la matrice a été altérée par lecture de la matrice en fonction de la somme de vérification et par vérification du fait que des données invalides sont lues.

23. Système de traitement selon la revendication 22, comprenant en outre un dispositif de comparaison du premier sous-ensemble décodé de données au second sous-ensemble de données.

24. Unité de traitement selon la revendication 23, comprenant en outre un dispositif destiné à créer un signal de sortie indiquant l'authenticité de l'article auto-vérificateur (104).

25. Système de traitement selon la revendication 22, dans lequel l'unité de traitement est en outre destinée à transformer l'ensemble reçu de données en une image numérique en mode points, et à séparer sélectivement l'image numérique en mode points en plusieurs régions dans lesquelles une première région contient le premier sous-ensemble codé de données et une seconde région contient le second sous-ensemble de données.

26. Système de traitement selon la revendication 25, dans lequel la première région et la seconde région comprennent chacune un sous-ensemble de données biométriques (101) et l'unité de traitement est en outre destinée à transformer le sous-ensemble de données biométriques de la première région (101) et le sous-ensemble de données biométriques de la seconde région (101) à un premier format de données.

27. Système de traitement selon la revendication 24, dans lequel la première région et la seconde région comprennent chacune un sous-ensemble de données de texte (102), et l'unité de traitement est en outre destinée à transformer le sous-ensemble de données de texte de la première région (102) et le sous-ensemble de données de texte de la seconde région (102) à un premier format numérique.

28. Système de traitement selon la revendication 22, comprenant en outre un dispositif destiné à afficher le premier sous-ensemble décodé de données.

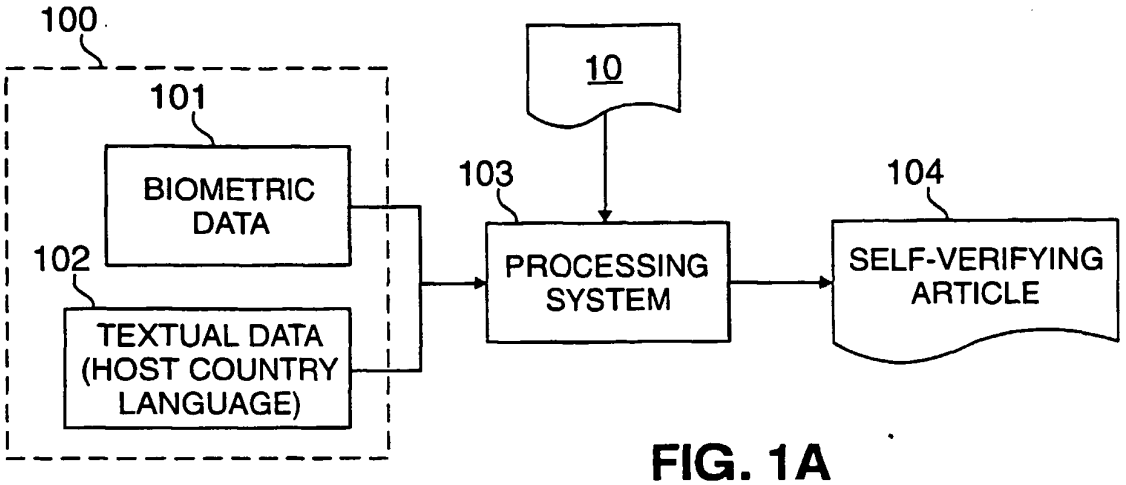
100
101
BIOMETRIC DATA
102
TEXTUAL DATA (HOST COUNTRY LANGUAGE)
10
103
PROCESSING SYSTEM
104
SELF-VERIFYING ARTICLE

FIG. 1A

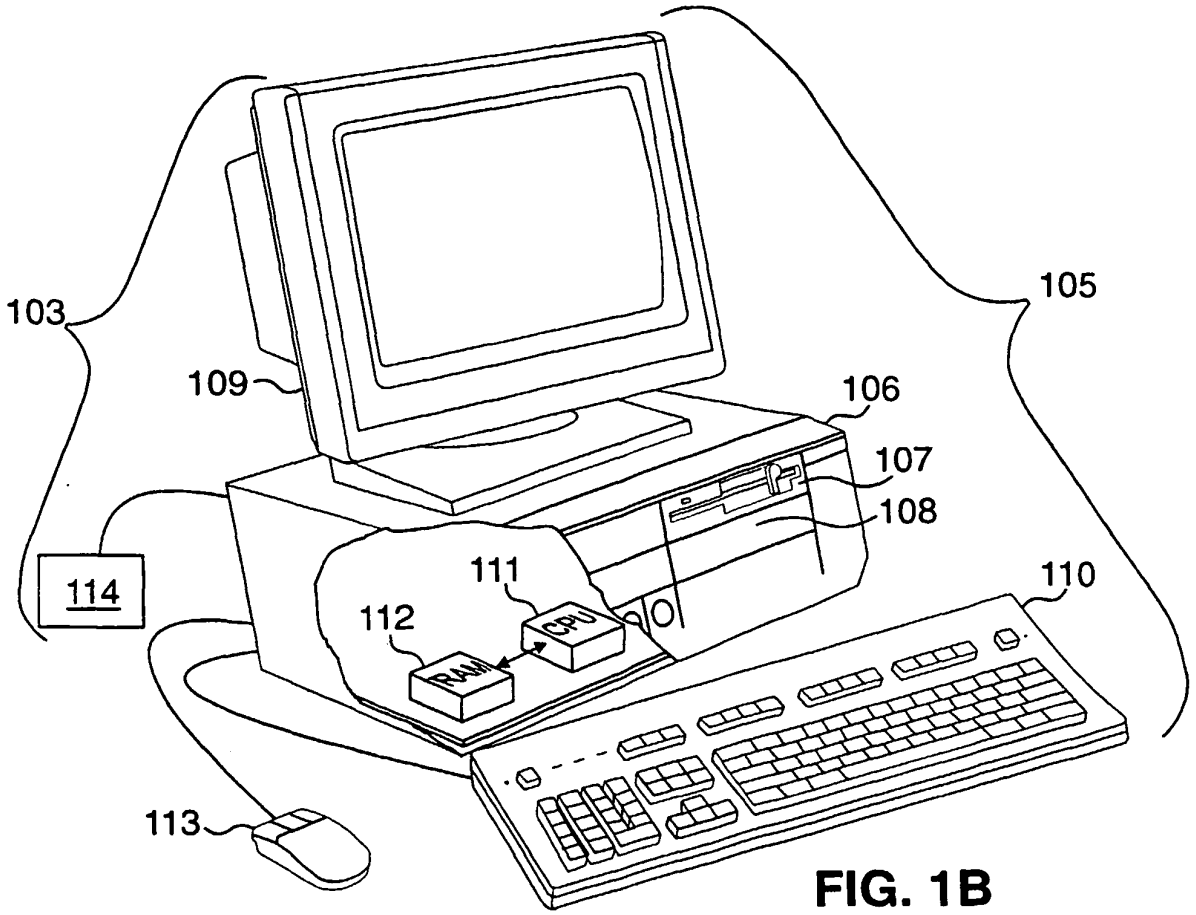
103
105
109
106
107
108
114
111
110
112
CPU
RAM
113

FIG. 1B

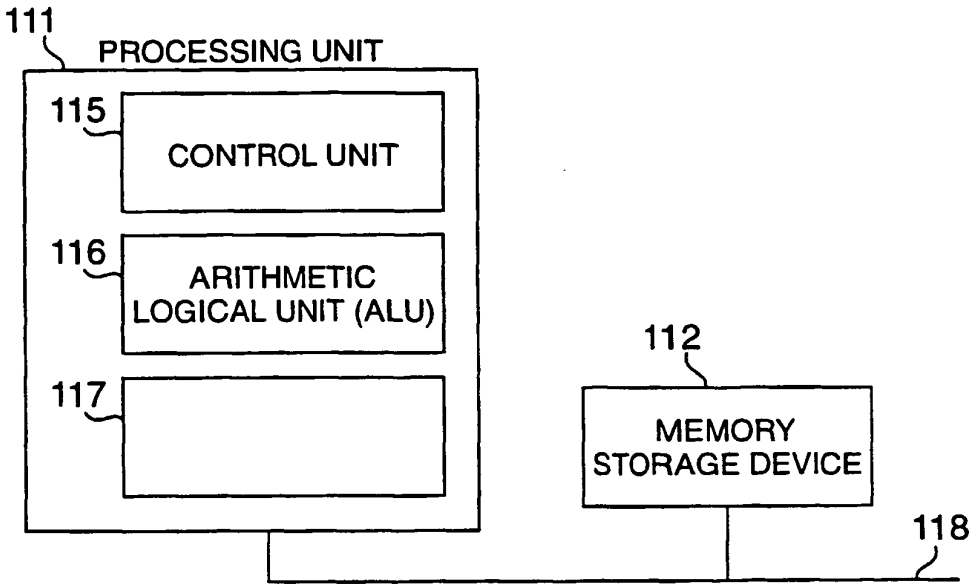
111
PROCESSING UNIT
115
CONTROL UNIT
116
ARITHMETIC LOGICAL UNIT (ALU)
117
112
MEMORY STORAGE DEVICE
118

FIG. 1C

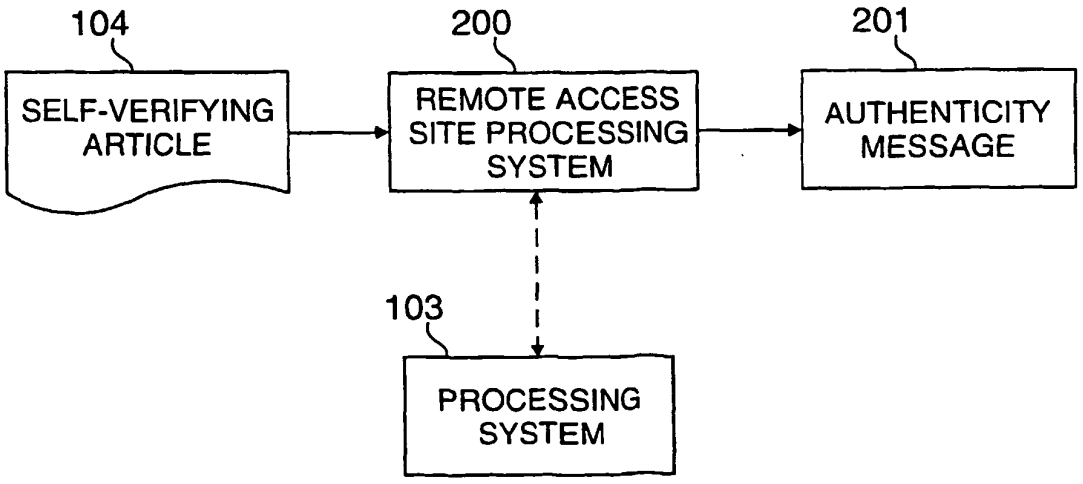
104
SELF-VERIFYING ARTICLE
200
REMOTE ACCESS SITE PROCESSING SYSTEM
201
AUTHENTICITY MESSAGE
103
PROCESSING SYSTEM

FIG. 2A

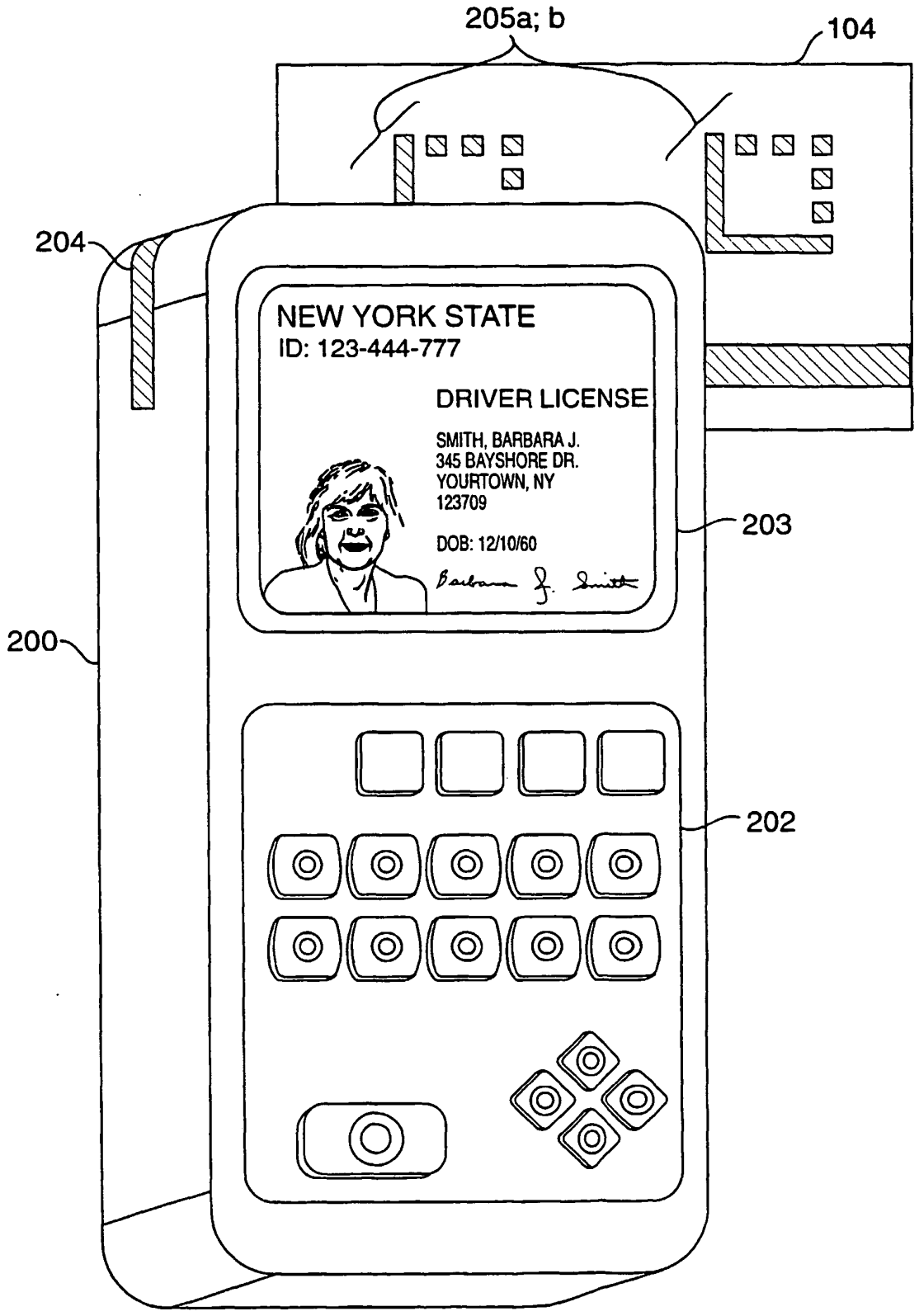
205a; b
104
204
NEW YORK STATE
ID: 123-444-777
DRIVER LICENSE
SMITH, BARBARA J.
345 BAYSHORE DR.
YOURTOWN, NY
123709
DOB: 12/10/60
203
200
202

FIG. 2B

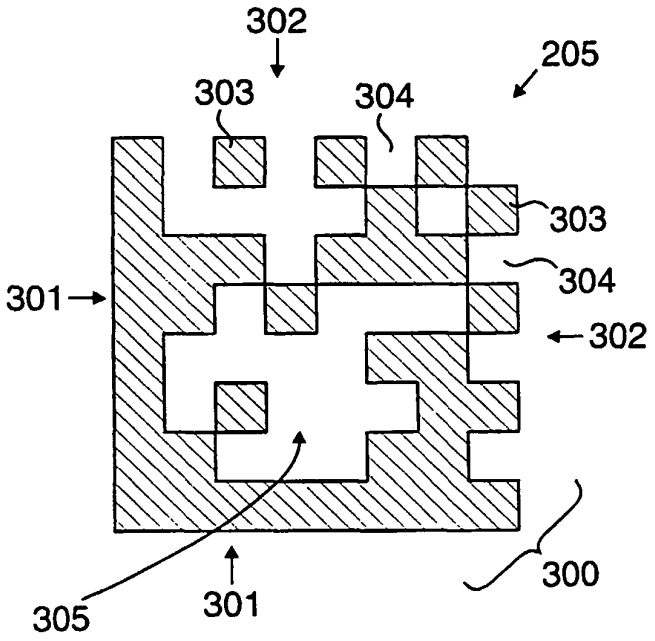
302
205
303
304
303
304
301
302
305
301
300

FIG. 3

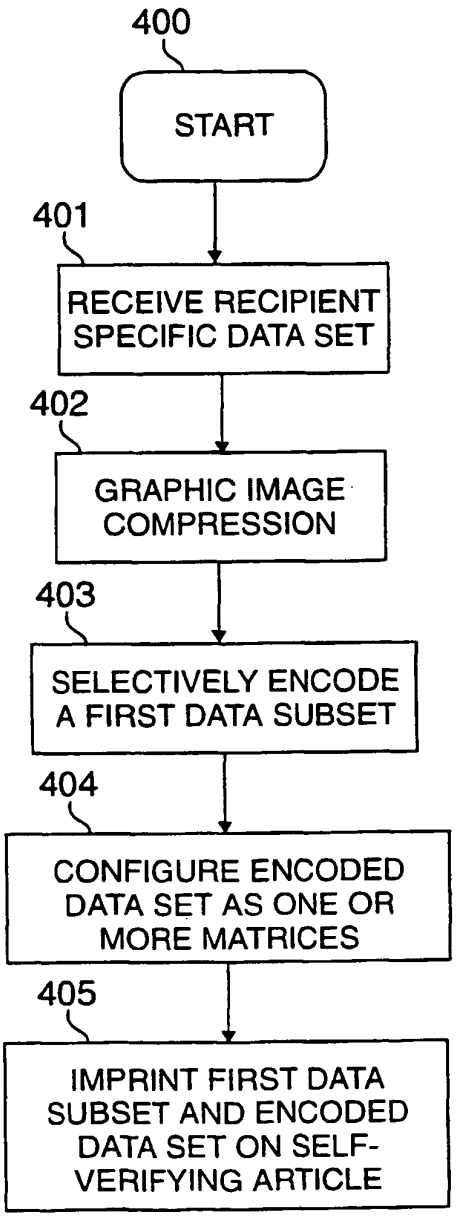
400
START
401
RECEIVE RECIPIENT SPECIFIC DATA SET
402
GRAPHIC IMAGE COMPRESSION
403
SELECTIVELY ENCODE A FIRST DATA SUBSET
404
CONFIGURE ENCODED DATA SET AS ONE OR MORE MATRICES
405
IMPRINT FIRST DATA SUBSET AND ENCODED DATA SET ON SELF-VERIFYING ARTICLE

FIG. 4A

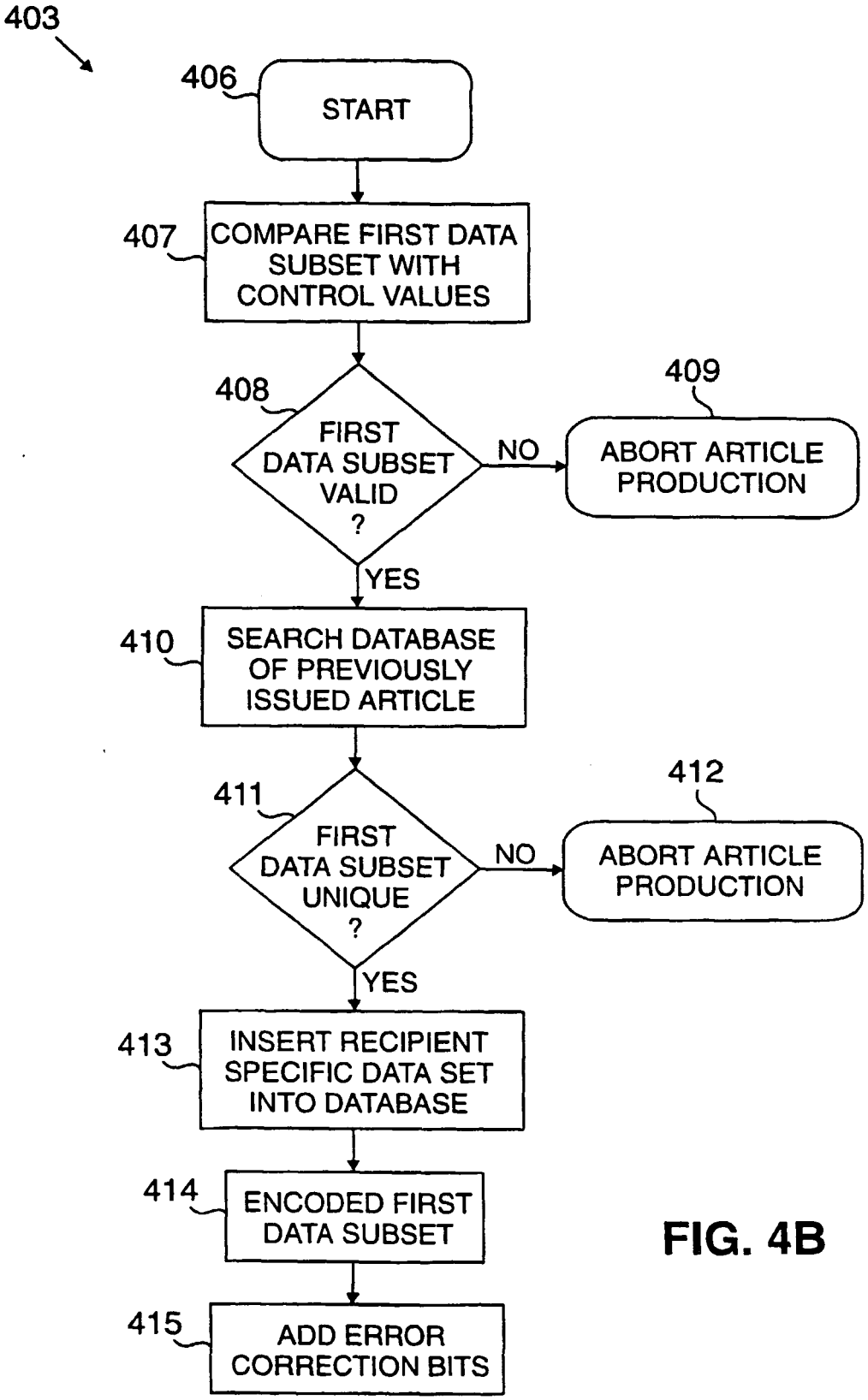
403
406
START
407
COMPARE FIRST DATA SUBSET WITH CONTROL VALUES
408
FIRST DATA SUBSET VALID ?
NO
409
ABORT ARTICLE PRODUCTION
YES
410
SEARCH DATABASE OF PREVIOUSLY ISSUED ARTICLE
411
FIRST DATA SUBSET UNIQUE ?
NO
412
ABORT ARTICLE PRODUCTION
YES
413
INSERT RECIPIENT SPECIFIC DATA SET INTO DATABASE
414
ENCODED FIRST DATA SUBSET
415
ADD ERROR CORRECTION BITS

FIG. 4B

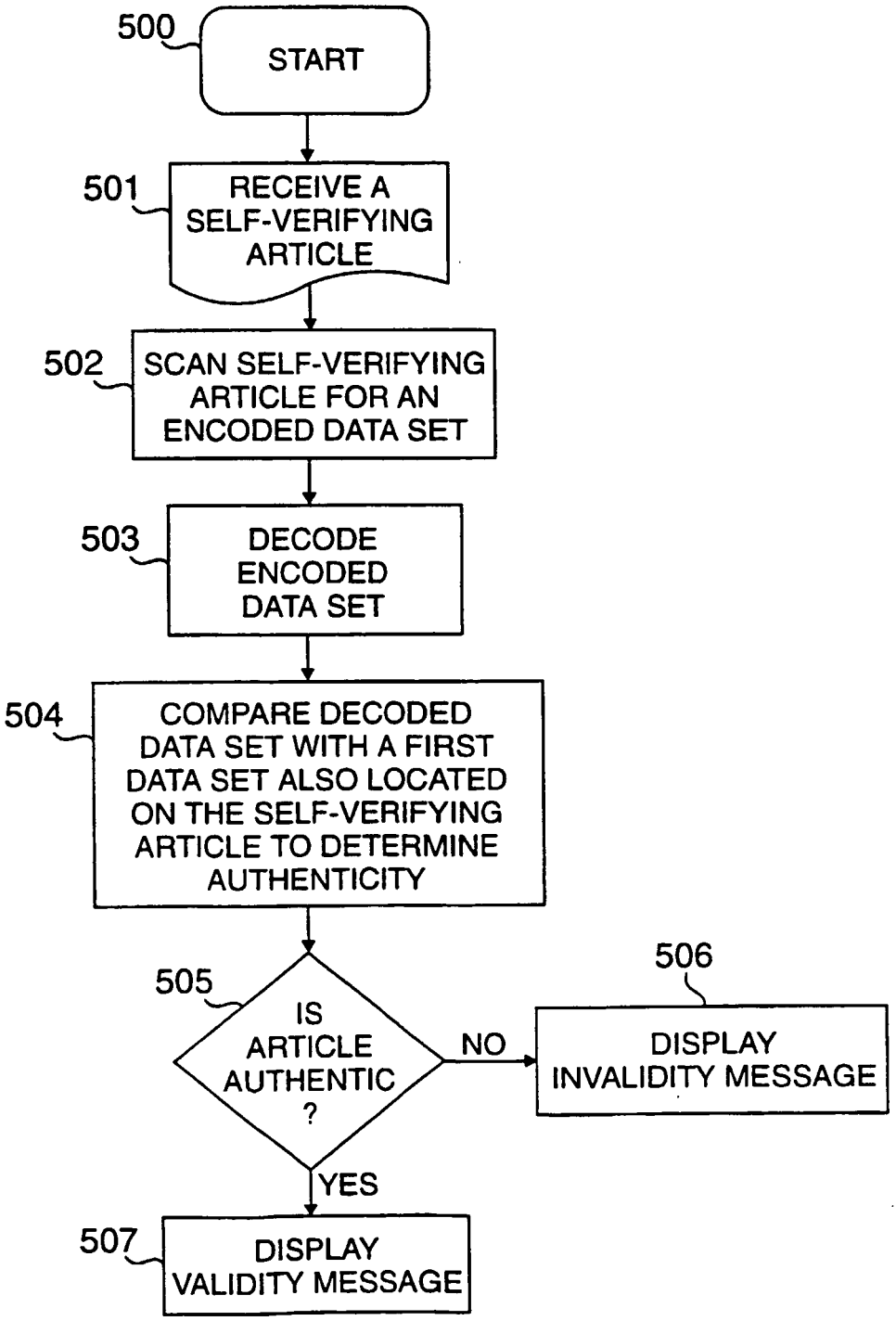
500
START
501
RECEIVE A SELF-VERIFYING ARTICLE
502
SCAN SELF-VERIFYING ARTICLE FOR AN ENCODED DATA SET
503
DECODE ENCODED DATA SET
504
COMPARE DECODED DATA SET WITH A FIRST DATA SET ALSO LOCATED ON THE SELF-VERIFYING ARTICLE TO DETERMINE AUTHENTICITY
505
IS ARTICLE AUTHENTIC ?
NO
506
DISPLAY INVALIDITY MESSAGE
YES
507
DISPLAY VALIDITY MESSAGE

FIG. 5