



(11) **EP 1 684 240 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Description Paragraph(s) 7, 8

(51) Int Cl.:
G07D 11/00 (2006.01) **G07F 7/10** (2006.01)
G07F 7/08 (2006.01) **H04L 9/32** (2006.01)

(48) Corrigendum issued on:
15.09.2010 Bulletin 2010/37

(45) Date of publication and mention
of the grant of the patent:
14.04.2010 Bulletin 2010/15

(21) Application number: **05018697.2**

(22) Date of filing: **29.08.2005**

(54) **Processing data transfer method in sheet processing apparatus**

Methode zur Übertragung von Bearbeitungsdaten in einer Blattverarbeitungsvorrichtung

Procédé de transfert de données de traitement dans un dispositif de traitement de feuilles

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

(30) Priority: **19.01.2005 JP 2005011749**

(43) Date of publication of application:
26.07.2006 Bulletin 2006/30

(73) Proprietor: **KABUSHIKI KAISHA TOSHIBA**
Tokyo 105-8001 (JP)

(72) Inventor: **Shishikura, Masahiro**
Intellectual Property Div.
Tokyo 105-8001 (JP)

(74) Representative: **Kramer - Barske - Schmidtchen**
European Patent Attorneys
Landsberger Strasse 300
80687 München (DE)

(56) References cited:
EP-A- 0 112 944 EP-A- 0 823 694
EP-A- 1 286 314 DE-A1- 4 442 357
US-A- 4 747 050 US-A1- 2004 059 676

- **PATENT ABSTRACTS OF JAPAN** vol. 2003, no. 01, 14 January 2003 (2003-01-14) & JP 2002 260140 A (TOSHIBA CORP), 13 September 2002 (2002-09-13)

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 684 240 B9

Description

[0001] This invention relates to a processing data transfer method in a sheet processing apparatus which separates securities such as banknotes into banknotes to be used again and banknotes which are not used again by checking the banknotes while the banknotes are being fed one by one, sealing every preset number of banknotes to be used again and cutting the banknotes which are not used again.

[0002] Conventionally, a sheet processing apparatus is configured by an equipment main body which processes paper sheet or the like and an information processing equipment which manages the equipment main body. The state and the number of paper sheets or the like which are processed by the equipment main body are checked and data of the processing result checked is managed by the information processing equipment (refer to Jpn. Pat. Appln. KOKAI Publication No. 2002-260140).

[0003] EP 1 286 314 discloses a method where a MAC is transmitted to a customer server along with the non-encrypted data. The server encrypts the non-encrypted data and compares the encrypted data and the MAC to determine whether they match.

[0004] In the above apparatus, in the case of data indicating the number (total sum) of cut sheets, data is enciphered in order to prevent data falsification.

[0005] For example, data (count information) of the number (total sum) of cut sheets by the equipment main body and MAC (Message Authentication Code) are transmitted to the information processing equipment. The information processing equipment stores the received count information and MAC into a database and transmits the count information to an IC card. Then, the IC card calculates the MAC based on the received count information by use of an enciphering key and returns the result of calculation as a response to the information processing equipment. Thus, the information processing equipment compares the MAC from the IC card with the MAC from the equipment main body to check whether or not they coincide with each other.

[0006] If the IC card and the password of the IC card are stolen, the following two problems will occur.

1) It becomes possible to attain a correct answer with respect to the MAC by supplying the count information to the IC card after falsifying the count information in the database. Then, if the MAC calculated by the equipment main body on the database is falsified by use of the MAC of the correct answer and subjected to the checking process again by use of the IC card, there occurs a problem that the result of the checking process becomes correct.

2) There occurs a problem that an enciphering key which is used to calculate the MAC can be estimated by sequentially changing data items supplied to the IC card.

[0007] An object of this invention is to prevent falsification of count information such as the number of sheets cut by the equipment main body without fail in a sheet processing apparatus which is configured by an equipment main body which processes paper sheets or the like and an information processing equipment which manages the equipment main body.

[0008] This is achieved by the processing data transfer method of the present invention as defined in claim 1.

[0009] Further advantageous features of the invention are defined in the sub-claims.

[0010] The invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a block diagram showing the schematic configuration of a paper-like sheet processing system, for illustrating one embodiment of this invention; FIG. 2 is an internal configuration view showing the schematic configuration of an equipment main body; FIG. 3 is a flowchart for illustrating the count information checking process; and FIG. 4 is a diagram for illustrating the count information checking process.

[0011] There will now be described an embodiment of this invention with reference to the accompanying drawings.

[0012] FIG. 1 is a system configuration diagram of a checking device used as a paper-like sheet processing system for overseas financial institutions.

[0013] That is, the paper-like sheet processing system has a plurality of sheet processing apparatuses 4 which are each configured by an equipment main body 1 which checks paper sheets (banknotes) supplied thereto and classifies the paper sheets based on the checking result and an information processing equipment (PC) 23 which manages the equipment main body by registering processing data of the processing result containing at least the number of classified sheets from the equipment main body 1 into a database. The plurality of sheet processing apparatuses 4 are connected via Ethernet 5 and a server 6 is connected to Ethernet 5.

[0014] The equipment main body 1 performs the following process. That is, it determines whether securities as paper sheets are true or false while they are being fed one by one. The true note or security is further subjected to an undamaged/damaged state determining process. Thus, the true note is separated into a practically undamaged note or excessively damaged note. Every preset number of practically undamaged notes are sealed and the excessively damaged notes are cut into pieces so as not to be used again. Thus, processing data of the processing result containing at least the number of sheets of securities which are subjected to the cutting process is output.

[0015] The equipment main body 1 has a main control section (control main unit) 11 which controls the whole

portion thereof. The main control section 11 realizes the function which permits the present apparatus to be operated so as to serve the preset purpose by collectively processing data items from a sub-control section 12 and determining control section 13 and finally transferring data with respect to the information processing equipment 3.

[0016] The information processing equipment 3 specifies the operation mode of the equipment main body 1 and operates the equipment main body. Further, it adequately monitors the operation state of each equipment main body 1, totalizes processing data output from the equipment main body 1 by use of the database 2 and prints the totalization result for each operation. The information processing equipment 3 is connected to the equipment main body 1 and IC card reader/writer 24 via USB (Universal Serial Bus) cables 21, 22.

[0017] The server 6 is connected to the information processing equipment 3 of the sheet processing apparatus 4 via Ethernet 5 and has a function of totalizing processing data by use of a database 7. Further, the server 6 performs the control operation for an IC card reader/writer 31 which will be described later. The server 6 is connected to the IC card reader/writer 31 via a USB (Universal Serial Bus) cable 32.

[0018] The schematic configuration of the equipment main body 1 is explained with reference to FIG. 2.

[0019] That is, the equipment main body 1 configured to process a preset number of paper sheets, for example, 1000 paper sheets as one unit. On the right end portion of the equipment main body 1, a sheet inserting unit 42 which automatically and sequentially inserts paper sheets in a stacked state for every 1000 sheets is provided.

[0020] The equipment main body 1 includes a fetching section 44 which sequentially fetches inserted paper sheets or the like one by one, a feeding device 46 which feeds the fetched sheet along a preset feeding path 47, a determining section 48 which detects information such as a pattern, dimension and feeding pitch from the sheet which is now being fed, a separating section 50 which selectively sets the feeding direction of the sheet according to the detection result, a storing section 52 which stores the thus separated sheets, a sealing section 54 which seals the stored paper sheets or the like for every preset number of sheets, and an invalidating section (cutting section) 53 which cuts and receives the paper sheets to be discarded.

[0021] A supply device 41 is provided near the fetching section 44. The supply device 41 receives the paper sheet P inserted from the inserting unit 42 and supplies the paper sheet to the fetching section 44. An attraction rotation roller 44a of the fetching section 44 fetches the paper sheets P one by one at preset pitches and transfers the paper sheet to the feeding device 46. The feeding device 46 is configured by a plurality of conveyor belts, driving pulleys, driving motors and the like arranged along the preset feeding path 47.

[0022] The determining section 48 includes a stacked-state detecting unit which detects a stacked state of the paper sheets P which are being fed, a reading unit which reads a pattern attached to the paper sheet P and a counter unit which counts the number of paper sheets P. The above units are arranged along the feeding path 47.

[0023] The paper sheets P which are subjected to the counting process, pattern reading process and length detecting process in the determining section 48 are classified into a plurality of types, for example, four types of paper sheets according to the detection result. Thus, the paper sheets are classified and stored for each type. A separating section 50 has three distribution gates 50a, 50b, 50c provided along the feeding path 47. The feeding path for the paper sheet is switched by selectively switching each gate position and the paper sheet is guided to a corresponding storage portion of a storing section 52 according to the type of the paper sheet.

[0024] The storing section 52 has two storing units 52a, 52b corresponding to the types of the paper sheets. A sealing section 54 includes sealing units 54a, 54b (paper sheet sealing units) (which are hereinafter simply referred to as sealing units) respectively arranged below the storing units 52a, 52b, a bundle sealing section 49 and a bundle packaging section 51. The invalidating section 53 includes a shredder and discarding box 53c and configures a number-of-sheets processing device.

[0025] With the above configuration, the count information checking process is explained with reference to the flowchart of FIG. 3 and a flow of information shown in FIG. 4.

[0026] First, a paper sheet is checked by use of the equipment main body 1 (ST1). That is, the equipment main body 1 determines whether the security is true or false while feeding the securities as paper sheets one by one. Further, it determines the true note or security as a practically undamaged note or excessively damaged note by subjecting the true note to an undamaged/damaged state determining process. Then, every preset number of practically undamaged notes are sealed and the excessively damaged notes are cut into pieces so as not to be used again. Thus, processing data of the processing result containing at least the number of sheets of securities which are subjected to the cutting process is output.

[0027] The main control section 11 forms count information and forms a MAC by use of the total sum of count information, date, time, count value and enciphering key stored in an internal memory (not shown) (ST2). The main control section 11 transmits the total sum of count information, date, time, count value and MAC to the information processing equipment 3 (ST3). The information processing equipment 3 stores count information transmitted from the main control section 11 into the database of the information processing equipment 3 and stores the count information into the database 7 of the server 6 (ST4).

[0028] Further, when the count information is checked

in the information processing equipment 3 after the end of the operation, the information processing equipment 3 transmits the total sum of count information, date, time, count value and MAC to the IC card by use of the IC card reader/writer 24 (ST5).

[0029] Thus, the IC card calculates a MAC by use of the total sum of count information, date, time, count value and the like by using an enciphering key (which is the same as the enciphering key of the main control section 11) stored in the internal memory. Then, it compares the MAC transmitted from the information processing equipment 3 with the calculated MAC by use of an internal control element and outputs the comparison result as a checking result (ST6). The checking result (Yes/No) from the IC card is transmitted to the information processing equipment 3 via the IC card reader/writer 24 (ST7). As a result, the information processing equipment 3 displays the checking result (ST8).

[0030] Further, like the information processing equipment 23, the count information can be checked in the server 6 by use of an IC card C.

[0031] As described above, the security of cutting data in the paper sheet checking equipment can be enhanced by calculating a MAC based on the cutting data. In the paper sheet checking equipment, falsification of count information is prevented by making the MAC calculated in the IC card invisible from the exterior.

[0032] The following effects can be expected in the paper sheet checking equipment. Since the MAC calculated by the IC card is made invisible from the exterior of the IC card, a MAC of a correct answer cannot be calculated by use of the IC card even if count data in the database of the PC is falsified.

[0033] Therefore, the checking result always becomes "No" if data is falsified and the checking process is performed by use of the IC card. Further, it becomes possible to prevent estimation of the enciphering key used to calculate a MAC by sequentially changing data to be transmitted to the IC card. In addition, even when the IC card and the password thereof are stolen, falsification of the count information can be prevented.

[0034] As a result, falsification of data by enciphering the number (total sum) of cut sheets in the paper sheet checking equipment can be prevented.

Claims

1. A processing data transfer method in a sheet processing apparatus configured by an equipment main body (1) which processes sheets and an information processing equipment (3) which manages the equipment main body (1), comprising transmitting (ST3) count information attained by the equipment main body (1) and a first MAC (Message Authentication Code) formed by use of the count information and an enciphering key to the information processing equipment (3; 23),

registering (ST4) the count information and the first MAC received by the information processing equipment (3; 23) into a database of the information processing equipment (3; 23) and transmitting the same from the information processing equipment (3; 23) to an IC card (C),

in the IC card (C), calculating (ST6) a second MAC by use of the count information received from the information processing equipment (3; 23) and the same enciphering key, which was used when forming the first MAC, comparing (ST6) the thus calculated second MAC with the first MAC from the equipment main body (1) and returning (ST7) a response indicating whether the compared first and second MACs coincide with each other to the information processing equipment (3; 23), and permitting the information processing equipment (3; 23) to output (ST8) the comparison result of the first and second MACs from the IC card as a checking result indicating that processing has been executed correctly when the first and second MACs coincide with each other, and indicating that processing has not been executed correctly when the first and second MACs do not coincide with each other.

2. The method according to claim 1, wherein the count information is the number of sheets which are determined not to be used again, subjected to a cutting process and set into an unusable state.
3. The method according to claim 1, wherein the count information contains at least one of the total sum of count information, date, time and count value.
4. The processing data transfer method according to any of claims 1 to 3 performed in a sheet processing apparatus configured by an equipment main body (1) which checks sheets supplied thereto and classifies the sheets based on the checking result and an information processing equipment (3) which manages the equipment main body (1) by registering processing data of the checking result containing at least the number of classified sheets from the equipment main body (1).
5. The method according to claim 4, wherein the processing result contains the number of sheets which are subjected to a cutting process when the sheets which are determined not to be used again by the sheet checking process are subjected to the cutting process and set into an unusable state.

Patentansprüche

1. Verarbeitungsdatenübertragungsverfahren in einer Blattverarbeitungsvorrichtung, die konfiguriert ist durch einen Einrichtungshauptkörper (1), der Blätter

verarbeitet, und durch eine Informationsverarbeitungseinrichtung (3), die den Einrichtungshauptkörper (1) verwaltet, mit

Übertragen (ST3) von Zählinformation, die durch den Einrichtungshauptkörper (1) gewonnen wird, und von einem ersten MAC (Nachrichtenauthentifizierungscode), der durch Verwendungen der Zählinformation und eines Verschlüsselungsschlüssels gebildet wird, an die Informationsverarbeitungseinrichtung (3; 23),

Registrieren (ST4) der Zählinformation und des ersten MAC, die von der Informationsverarbeitungseinrichtung (3; 23) empfangen werden, in einer Datenbank der Informationsverarbeitungseinrichtung (3; 23), und selbige von der Informationsverarbeitungseinrichtung (3; 23) an eine IC-Karte (C) übertragen,

Berechnen (ST6) eines zweiten MAC in der IC-Karte (C) durch Verwenden der Zählinformation, die von der Informationsverarbeitungseinrichtung (3; 23) empfangen wird, und des gleichen Verschlüsselungsschlüssels, der bei der Bildung des ersten MAC verwendet wurde, Vergleichen (ST6) des folglich berechneten zweiten MAC mit dem ersten MAC von dem Einrichtungshauptkörper (1), und Zurückgeben (ST7) einer Antwort, die angibt, ob die verglichenen ersten und zweiten MACs übereinstimmen, an die Informationsverarbeitungseinrichtung (3; 23) und der Informationsverarbeitungseinrichtung (3; 23) erlauben, das Vergleichsergebnis der ersten und zweiten MACs von der IC-Karte als ein Prüfergebnis auszugeben (ST8), das angibt, dass die Verarbeitung korrekt durchgeführt wurde, wenn der erste MAC und der zweite MAC übereinstimmen, und das angibt, dass die Verarbeitung nicht korrekt durchgeführt worden ist, wenn der erste und der zweite MAC nicht übereinstimmen.

2. Verfahren nach Anspruch 1, bei dem die Zählinformation gleich der Anzahl von Blättern ist, die als nicht erneut zu verwenden bestimmt, einem Schneideprozess unterworfen und in einen nicht verwendbaren Zustand gesetzt werden.
3. Verfahren nach Anspruch 1, bei dem die Zählinformation von einer Zählinformationssumme, einem Datum, einer Zeit und einem Zählwert mindestens eines enthält.
4. Verarbeitungsdatenübertragungsverfahren nach einem der Ansprüche 1 bis 3, das in einer Blattverarbeitungsvorrichtung durchgeführt wird, die durch einen Einrichtungshauptkörper (1) konfiguriert ist, der an ihn gelieferte Blätter prüft und die Blätter basierend auf dem Überprüfungsergebnis klassifiziert, und durch eine Informationsverarbeitungseinrichtung (3), die den Einrichtungshauptkörper (1) verwaltet durch Registrieren von Verarbeitungsdaten

des Prüfergebnisses, enthaltend mindestens die Anzahl der von dem Einrichtungshauptkörper (1) klassifizierten Blättern.

5. Verfahren nach Anspruch 4, bei dem das Verarbeitungsergebnis die Anzahl von Blättern enthält, die einem Schneideprozess unterworfen werden, wenn die Blätter, die als nicht erneut zu verwenden durch den Blattüberprüfungsprozess bestimmt worden sind, dem Schneideprozess unterworfen und in einen nicht verwendbaren Zustand gesetzt werden.

Revendications

1. Procédé de transfert de données de traitement dans un appareil de traitement de feuilles configuré par un corps principal d'équipement (1) qui traite des feuilles et un équipement de traitement d'information (3) qui gère le corps principal d'équipement (1), le procédé comprenant les étapes de :

transmission (ST3) à l'équipement de traitement d'information (3; 23) d'informations de compte atteint par le corps principal d'équipement (1) et d'un premier MAC (Code d'Authentification de Message) formé par l'utilisation des informations de compte et d'une clé de chiffrement, enregistrement (ST4) dans une base de données de l'équipement de traitement d'information (3; 23) des informations de compte et du premier MAC reçus par l'équipement de traitement d'information (3; 23) et transmission de ces éléments de l'équipement de traitement d'information (3; 23) à une carte à CI (C), dans la carte à CI (C), calcul (ST6) d'un second MAC à l'aide des informations de compte reçues par l'équipement de traitement d'information (3; 23) et de la même clé de chiffrement que celle qui a été utilisée lors de la formation du premier MAC, comparaison (ST6) du second MAC ainsi calculé au premier MAC par le corps principal d'équipement (1), et renvoi (ST7) à l'équipement de traitement d'information (3; 23) d'une réponse indiquant si les premier et second MAC comparés coïncident l'un avec l'autre, et autorisation de l'équipement de traitement d'information (3; 23) à émettre (ST8) le résultat de la comparaison des premier et second MAC par la carte à CI sous la forme d'un résultat de contrôle indiquant que le traitement a été exécuté correctement lorsque les premier et second MAC coïncident l'un avec l'autre et indiquant que le traitement n'a pas été exécuté correctement lorsque les premier et second MAC ne coïncident pas l'un avec l'autre.

2. Procédé selon la revendication 1, dans lequel les

informations de compte sont constituées du nombre de feuilles qui sont déterminées comme ne devant pas être réutilisées, soumises à une opération de découpe et rendues inutilisables.

5

3. Procédé selon la revendication 1, dans lequel les informations de compte contiennent au moins l'un de la somme totale des informations de compte, la date, l'heure et la valeur du compte.

10

4. Procédé de transfert de données de traitement selon l'une quelconque des revendications 1 à 3, exécuté dans un appareil de traitement de feuilles configuré par un corps principal d'équipement (1) qui contrôle les feuilles qui lui sont amenées et qui classe les feuilles en fonction du résultat de contrôle et un équipement de traitement d'information (3) qui gère le corps principal d'équipement (1) en enregistrant des données de traitement du résultat de contrôle contenant au moins le nombre de feuilles classées par le corps principal d'équipement (1).

15

20

5. Procédé selon la revendication 4, dans lequel le résultat de traitement contient le nombre de feuilles qui sont soumises à une opération de découpe lorsque les feuilles qui ont été déterminées comme ne devant pas être réutilisées par le processus de contrôle de feuilles sont soumises à l'opération de découpe et rendues inutilisables.

25

30

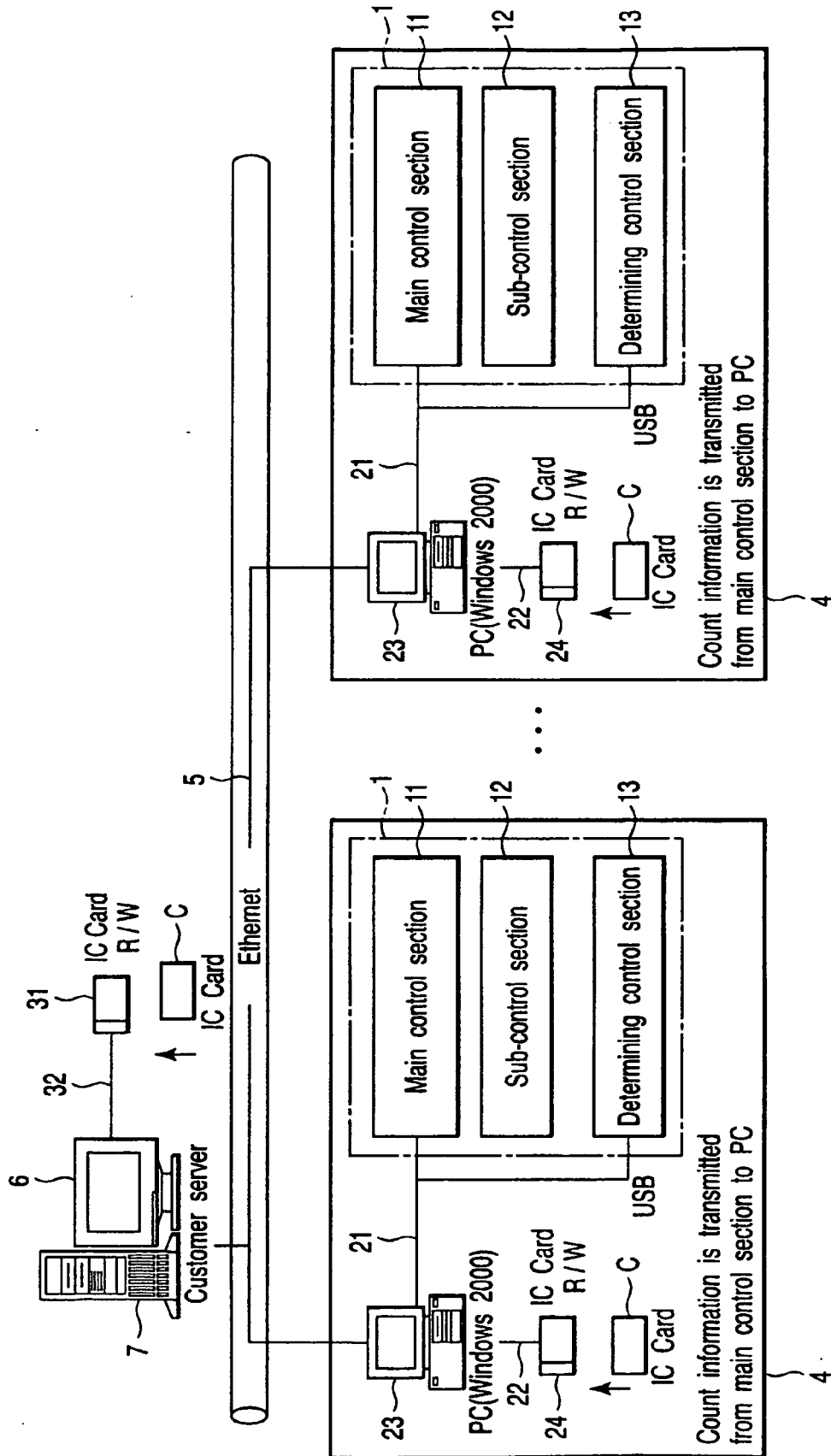
35

40

45

50

55



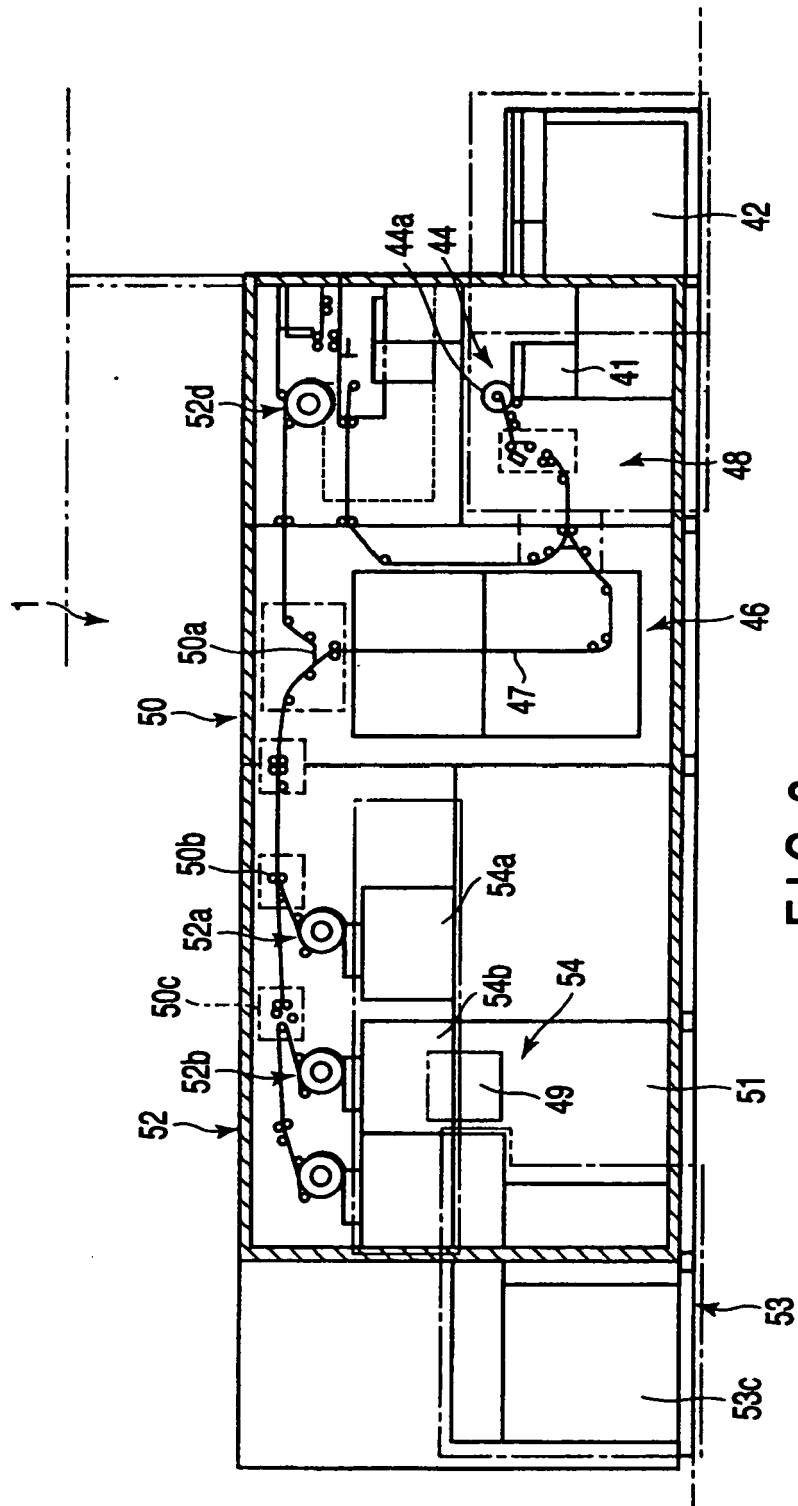


FIG. 2

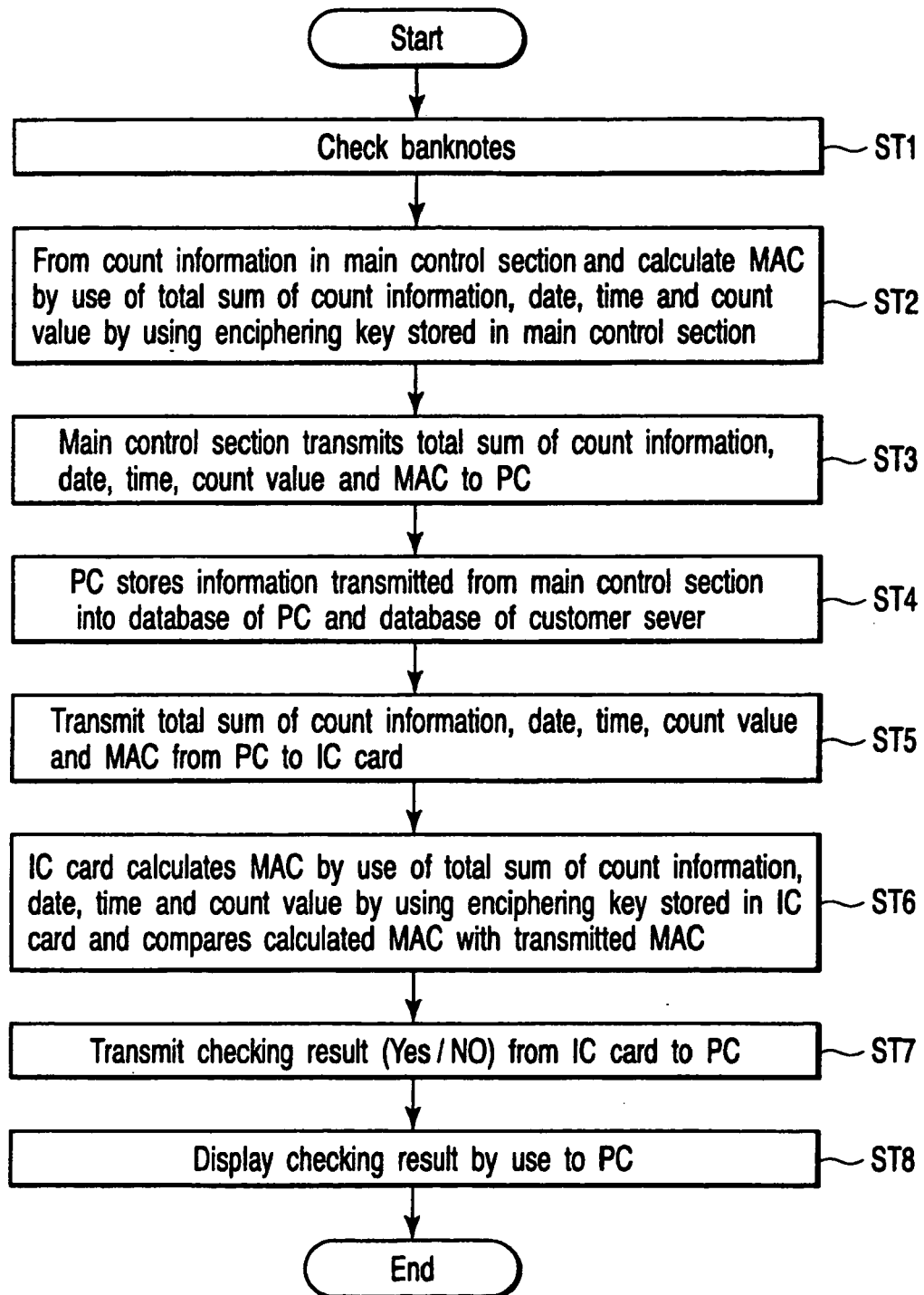


FIG. 3

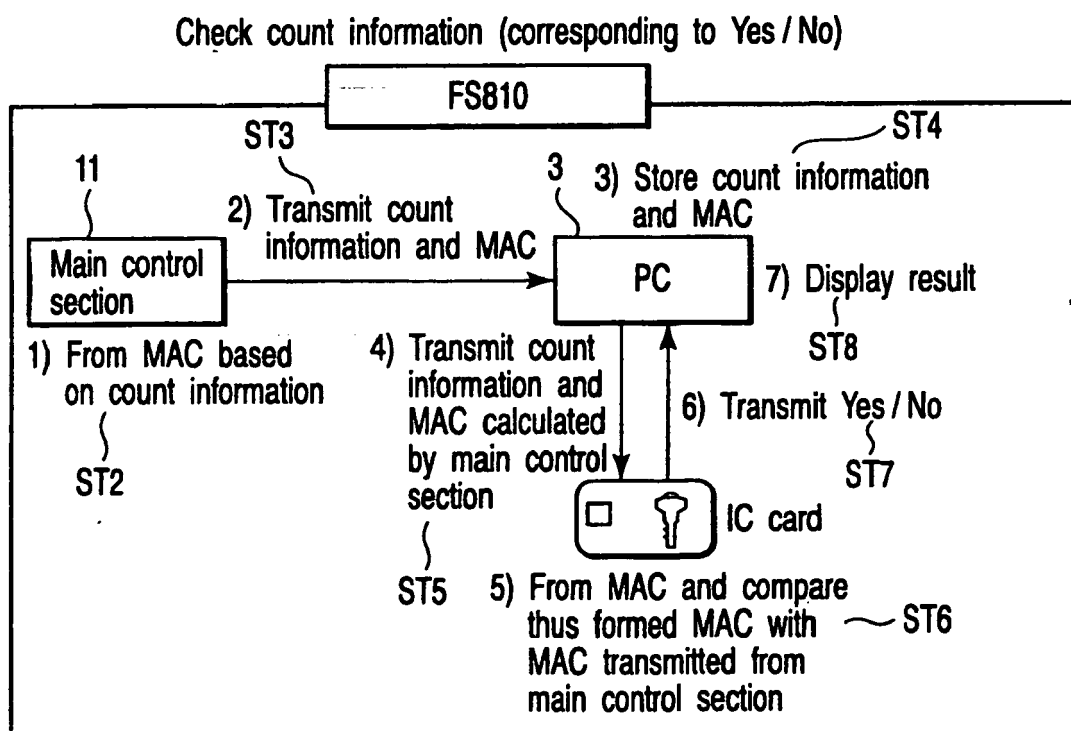


FIG. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 2002260140 A [0002]
- EP 1286314 A [0003]