



Europäisches Patentamt
European Patent Office
Office européen des brevets



Veröffentlichungsnummer: **0 453 930 A2**

12

EUROPÄISCHE PATENTANMELDUNG

21 Anmeldenummer: **91106069.7**

51 Int. Cl.⁵: **G07D 7/00**

22 Anmeldetag: **16.04.91**

30 Priorität: **27.04.90 DE 4013585**

W-8000 München 70(DE)

43 Veröffentlichungstag der Anmeldung:
30.10.91 Patentblatt 91/44

72 Erfinder: **Hell, Wilhelm**
Lilienthalstrasse 10
W-8905 Mering(DE)

84 Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI LU NL SE

71 Anmelder: **GAO Gesellschaft für Automation
und Organisation mbH**
Euckenstrasse 12

74 Vertreter: **Klunker . Schmitt-Nilson . Hirsch**
Winzererstrasse 106
W-8000 München 40(DE)

54 **Verfahren zur Überprüfung der ordnungsgemässen Bearbeitung von Banknoten.**

57 Die Erfindung betrifft ein Verfahren zur Überprüfung der ordnungsgemässen Bearbeitung von Banknoten in automatischen Banknoten-Sortieranlagen, die bestimmte Geldmengen nach vorgebbaren Kriterien in unterschiedliche Kategorien sortiert, bei der Teilmengen gegebenenfalls zerstört werden und bei der nach der Bearbeitung einer vorgebbaren Geldmenge oder nach einer bestimmten Zeiteinheit ein

Protokoll erstellt wird, in dem unter anderem Informationen über die bearbeiteten Banknoten registriert sind, und daß zusätzlich auf dem Protokoll wenigstens eine aus vorgebbaren Protokolldaten errechnete Echtheitskennzeichnung vorgesehen ist, die in einer eindeutigen Beziehung zu den in die Berechnung einbezogenen Daten steht.

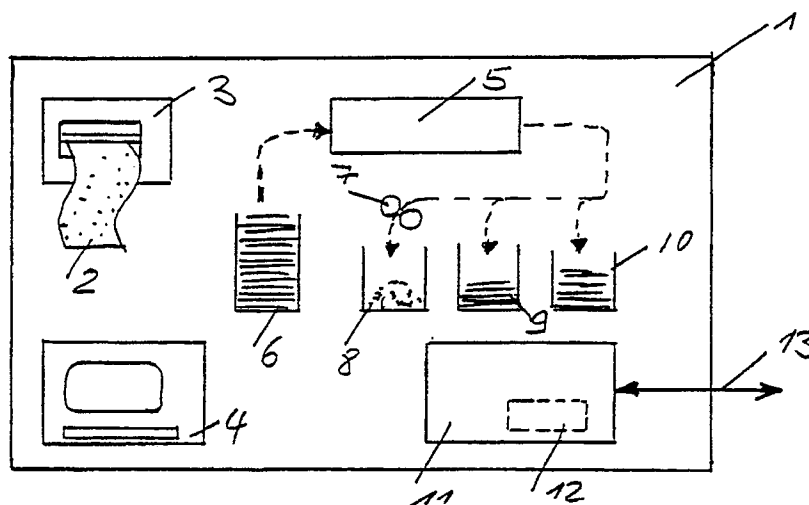


Fig. 1

EP 0 453 930 A2

Die Erfindung betrifft ein verfahren zur Überprüfung der ordnungsgemäßen Bearbeitung von Banknoten in automatischen Banknoten-Sortieranlagen, die bestimmte Geldmengen nach vorgebbaren Kriterien in unterschiedliche Kategorien sortiert, bei der Teilmengen gegebenenfalls zerstört werden und bei der nach der Bearbeitung einer vorgebbaren Geldmenge oder nach einer bestimmten Zeiteinheit ein Protokoll erstellt wird, in dem unter anderem Informationen über die bearbeiteten Banknoten registriert sind.

Zur Sortierung von Banknoten werden seit längerem Automaten eingesetzt, die automatisch oder auch manuell zugeführte Banknoten vereinzeln, der Reihe nach durch ein Sensorsystem führen und je nach Aufgabenstellung und Sensorergebnis nach vorgebbaren Kriterien in unterschiedliche Kategorien sortieren.

Ein solcher Automat ist beispielsweise aus der DE-PS 27 60 269 bekannt. Eine wesentliche Aufgabe dieses bekannten Sortierautomaten besteht darin, aus dem Geldumlauf zurückfließende Banknoten in für den weiteren Umlauf brauchbare und nicht brauchbare Banknoten zu sortieren. In eine dritte Kategorie werden Banknoten sortiert, die beispielsweise falschgeldverdächtig, nicht identifizierbar oder aus anderen Gründen nicht sortierbar sind. Die für den weiteren Umlauf als nicht brauchbar identifizierten Noten müssen zuverlässig zerstört werden, was beispielsweise dadurch geschehen kann, daß die Noten einen in der Sortiermaschine integrierten Schredderbaustein passieren, der jede Note in so kleine Schnipsel zerteilt, daß daraus eine Wiederherstellung von Noten unmöglich ist.

Die Geldbearbeitung auf der Ebene der Sortiermaschine läßt sich grob in drei Schritte untergliedern. Der Bediener der Maschine erhält zu Beginn seiner Schicht ein bestimmtes Geldvolumen, dessen Erhalt er quittiert.

Die erhaltene Geldmenge wird der Maschine zugeführt und beispielsweise in die genannten Kategorien sortiert. Nach Beendigung der Schicht übergibt der Bediener die sortierten Geldmengen zusammen mit einem alle relevanten Vorgänge protokollierenden Ausdruck einer die Geldbearbeitung weiterführenden Institution.

Wie in der DE-OS 27 60 269 ausführlich beschrieben, ist die Sortiermaschine mit einer Druckeinrichtung versehen, über die unter anderem auch ein sogenanntes Schichtprotokoll ausgedruckt werden kann. In diesem Protokoll sind neben anderen Daten die Summen der in den vorgesehenen Kategorien abgelegten Banknoten registriert. Die Summe über alle Teilmengen in den Kategorien muß dem der Maschine zugeführten und vom Bediener quittierten Geldvolumen entsprechen. Anhand der Protokolldaten ist grundsätzlich eine Überprüfung der einzelnen Geldmengen durch beispielsweise

nochmaliges Nachzählen möglich, so daß keine Banknote unerkannt verschwinden kann. Diese einfache Form der Überprüfung ist allerdings bei zerstörten Noten nicht mehr möglich, so daß besonders bezüglich dieser Noten eine andere Form der Sicherheitsüberprüfung notwendig ist, um gegen mögliche Manipulationen geschützt zu sein.

Die Aufgabe der Erfindung besteht deshalb darin, beim Einsatz einer automatischen Banknotensortiermaschine mit integrierter Schalteinrichtung einen höchstmöglichen Schutz gegen Manipulation zu gewährleisten.

Das Wesentliche der Erfindung besteht darin, aus den zu schützenden Protokolldaten unter Verwendung eines kryptografischen Prozesses einen Wert zu errechnen, der auf dem Protokollauszug ein- oder auch mehrfach ausgedruckt wird. Diese Berechnung kann nur von autorisierten Stellen durchgeführt werden, die Kenntnis von dem kryptografischen Prozeß bzw. von den in diesen Prozeß einbezogenen Geheimnissen haben. Jede Verfälschung, Einfügung oder Entfernung von Protokolldaten führt zu einem anderen Echtheitswert, was bei einer Überprüfung auf einfache Weise feststellbar ist.

Gemäß einer bevorzugten Ausführungsform der Erfindung wird zur Absicherung der Protokolldaten ein Echtheitscode berechnet und zur Überprüfung der Echtheit des Protokolls dieser Code nach dem gleichen Verfahren erneut berechnet und mit dem früher ermittelten auf Identität geprüft.

Die Bildung von sogenannten Authentisierungs-codes ist in der Nachrichtenfernübertragung seit längerem bekannt. Die Anwendung dieses an sich bekannten Verfahrens bietet aber bei der Absicherung von Protokolldaten einer Banknotensortiervorrichtung eine technisch einfach zu realisierende Möglichkeit, gerade auch die Daten von zerstörten Noten, deren korrekte Bearbeitung nicht so ohne weiteres nachprüfbar ist, sehr wirkungsvoll gegen Manipulationen zu schützen. Selbstverständlich kann das Verfahren auch bei Sortiervorrichtungen ohne Schredderfunktion wirkungsvoll eingesetzt werden, um die Authentizität der erstellten Protokolle zu sichern.

Gemäß einer Weiterbildung der Erfindung werden zeitvariable Protokolldaten in die Berechnung der Echtheitskennzeichnung einbezogen, um Protokolle mit gleichen oder ähnlichen Sortiierungsergebnissen eindeutig voneinander unterscheiden zu können.

Die Berechnung des Authentisierungs-codes wird jeweils vor einem Protokollausdruck in einem entsprechenden Sicherheitsmodul der Sortiervorrichtung durchgeführt. Je nach den vereinbarten organisatorischen Richtlinien werden pro Schicht oder Bearbeitungszeitraum ein oder mehrere Protokolle mit den zugehörigen Echtheitscodes verse-

hen, die auch in der Maschine gespeichert werden können. Gespeicherte Echtheitscodes können am Folgetag oder auch später zu Kontrollzwecken nochmals überprüft werden.

Weitere Vorteile und Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen sowie aus der nachfolgenden Beschreibung eines Ausführungsbeispiels der Erfindung anhand der Figuren. Darin zeigen:

Fig. 1 eine Banknotensortiervorrichtung in grob schematisierter Form und

Fig. 2 den Auszug aus einem Protokoll.

Die Fig. 1 zeigt in stark schematisierter Form eine mögliche Konfiguration einer Sortiervorrichtung mit den wesentlichen Funktionselementen.

Die Banknoten werden aus einem Eingangsbehälter 6 vereinzelt, durch eine Sensorstrecke 5 geführt und abhängig vom Sensorergebnis unterschiedlichen Ausgangsbehältern 8, 9 oder 10 zugeführt. Im Behälter 8 werden die durch eine Shreddereinrichtung 7 zerstörten Banknoten gesammelt. Im Behälter 9 können für den weiteren Umlauf noch brauchbare Noten und im Behälter 10 sogenannte Handnacharbeitsnoten gesammelt werden. Letztere Noten sind vom Bediener der Maschine nochmals genau zu prüfen, da es sich beispielsweise um falschgeldverdächtige oder nicht identifizierbare Noten handelt. Über eine Konsole 4 ist der Dialog mit der Maschine möglich. Zum Ausdruck von Protokollen 2 über die Geldbearbeitung ist die Sortiermaschine mit einem Drucker 3 ausgerüstet.

Ein Beispiel eines solchen Protokolls ist in der Fig. 2 gezeigt. Je nach den organisatorischen Vorgaben können verschiedene Arten von Protokollen ausgedruckt werden, worauf hier aber nicht näher eingegangen werden soll.

Die Fig. 2 zeigt ein sogenanntes Schichtprotokoll, das ein Bediener nach der Abarbeitung eines bestimmten Geldvolumens ausdrucken läßt. Dieses Protokoll wird gemeinsam mit den bearbeiteten und in den genannten Kategorien sortierten Banknoten einer das Geld weiter bearbeitenden Institution übergeben.

Neben einer Datum- und Zeitangabe kann auf dem Protokoll die Maschinen-Nummer bzw. auch eine Ident-Nummer des Bedieners aufgezeichnet sein. Auf dem Protokoll sind außerdem die Summen der in den unterschiedlichen Kategorien (umlauffähige Noten kurz U-Noten genannt und Handnacharbeitsnoten kurz HN-Noten genannt) abgelegten Banknoten bzw. der zerstörten Noten (kurz Shr-Noten genannt) ausgedruckt. Die genannten Informationen stellen nur eine Auswahl der möglichen Protokolldaten dar. Zusätzlich zu den genannten Informationen ist nun gemäß der Erfindung auf dem Protokoll eine Echtheitskennzeichnung 15 vorgesehen, die aus allen oder aus einer bestimmten Auswahl von Protokolldaten über einen

kryptografischen Prozeß errechnet wird. Vorzugsweise wird man diejenigen Daten, die gegen Verfälschung gesichert werden sollen, in den Prozeß einbeziehen. In jedem Fall steht die Echtheitskennzeichnung in einem eindeutigen Zusammenhang zu den einbezogenen Daten. Jede Veränderung, Ergänzung oder Streichung von Daten führt zu einer anderen Echtheitskennzeichnung, womit jede Manipulation an den Protokolldaten sofort aufgedeckt wird.

Die Echtheitskennzeichnung kann in einem Sicherheitsmodul 12 der Steuer- und Recheneinheit 11 der Sortiervorrichtung berechnet werden. In diesem Modul befinden sich der Algorithmus bzw. die geheimen Schlüssel zur Berechnung der Kennzeichnung. Das Modul ist daher entsprechend gegen den nicht autorisierten Zugriff zu schützen. In die Berechnung der Echtheitskennzeichnung sollten zeitvariable Größen einbezogen werden, wie beispielsweise das Datum oder die Uhrzeit oder auch andere diesen Zweck erfüllende Werte, so daß jedes Protokoll ein Unikat darstellt. Die Echtheitskennzeichnung kann auf dem Protokoll mehrfach ausgedruckt werden, beispielsweise, wie in der Fig. 2 gezeigt, vor und nach den eigentlichen Protokolldaten.

Die Prüfung der Echtheit des Protokolls kann mit jedem Gerät durchgeführt werden, das über das in der Sortiermaschine implementierte Sicherheitsmodul 12 verfügt und mit dem entsprechenden Algorithmus bzw. Schlüssel geladen ist. Über eine Tastatur des Gerätes werden die in die Berechnung der Echtheitskennzeichnung einbezogenen Daten, wie beispielsweise die Summen der U-BN, der HN-BN, der Shr-BN manuell eingegeben. Das Sicherheitsmodul errechnet daraus die Echtheitskennzeichnung und zeigt diese auf einem Display an, so daß der Bediener die angezeigte Kennzeichnung mit der auf dem Protokoll ausgedruckten Kennzeichnung vergleichen kann. Bei Identität ist sichergestellt, daß die überprüften Protokolldaten unverfälscht sind. Trotz der Einfachheit sowohl der Erstellung der Echtheitskennzeichnung als auch der Überprüfung derselben wird mit dem erfindungsgemäßen Verfahren ein hohes Maß an Sicherheit erreicht, was die ordnungsgemäße Bearbeitung von Banknoten in automatischen Banknotensortieranlagen betrifft. Die Prüfung kann auch an der Schreddermaschine selbst durchgeführt werden, nachdem eine dafür vorgesehene Betriebsart über die Bedienerkonsole 4 angewählt wurde. Das Ergebnis wird auf dem Bildschirm der Bedienerkonsole angezeigt. Auf die Darstellung eines gesonderten Verifizierungsgerätes, das wenigstens das Sicherheitsmodul 12 und eine Bedienerkonsole 4 aufweist, wurde der Klarheit wegen verzichtet.

Die Prüfung der Echtheitskennzeichnung der Protokolldaten kann auch mit Hilfe eines Terminals

durchgeführt werden, das über die Schnittstelle 13 mit der Sortiermaschine 1 verbunden ist. Die notwendigen Daten werden dem Terminal übermittelt, woraus in einem entsprechenden Sicherheitsmodul des Terminals der Echtheitscode, wie oben geschildert, errechnet wird.

Die Echtheitskennzeichnungen mehrerer Protokolle können beispielsweise unter der Protokollnummer oder auch anderer geeigneter Daten in einem Speicher der Sortiermaschine abgelegt werden, so daß auch zu einem späteren Zeitpunkt noch Überprüfungen alter Protokolle möglich sind.

Patentansprüche

1. Verfahren zur Überprüfung der ordnungsgemäßen Bearbeitung von Banknoten in automatischen Banknoten-Sortieranlagen, die bestimmte Geldmengen nach vorgebbaren Kriterien in unterschiedliche Kategorien sortiert, bei der Teilmengen gegebenenfalls zerstört werden und bei der nach der Bearbeitung einer vorgebbaren Geldmenge oder nach einer bestimmten Zeiteinheit ein Protokoll erstellt wird, in dem unter anderem Informationen über die bearbeiteten Banknoten registriert sind, dadurch **gekennzeichnet**, daß zusätzlich auf dem Protokoll wenigstens eine aus vorgebbaren Protokolldaten errechnete Echtheitskennzeichnung vorgesehen ist, die in einer eindeutigen Beziehung zu den in die Berechnung einbezogenen Daten steht. 15
2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß das Echtheitskennzeichen zu Beginn und am Ende der Protokolldaten ausgedruckt ist. 20
3. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß in die Berechnung der Echtheitskennzeichnung ein zeitvariabler Parameter einbezogen wird. 25
4. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Berechnung der Echtheitskennzeichnung über einen kryprografischen Prozeß unter Einbeziehung geheimer Informationen durchgeführt wird, wobei der Algorithmus und die Geheiminformation in einem Sicherheitsmodul der Sortieranlage implementiert sind. 30
5. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Echtheitskennzeichen einer oder mehrerer Protokolle zusätzlich in der Sortiermaschine gespeichert werden. 35
6. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Überprüfung der Protokolldaten durch Nachberechnung des Echtheitskennzeichens und Vergleich mit dem auf dem Protokoll ausgedruckten Echtheitskennzeichen durchgeführt wird. 40
7. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß zur Prüfung des Protokolls die Protokolldaten manuell in eine von der Sortiermaschine unabhängige Recheneinrichtung eingegeben werden und das von der Recheneinrichtung ermittelte und angezeigte Ergebnis mit dem auf dem Protokoll ausgedruckten Echtheitskennzeichen verglichen wird. 45
8. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß zur Prüfung des Protokolls die Daten über die Schnittstelle einer mit der Sortiervorrichtung verbundenen Einheit zugeführt werden, die automatisch anhand der Daten die Nachberechnung und den Vergleich durchführt. 50

zeichnet, daß die Überprüfung der Protokolldaten durch Nachberechnung des Echtheitskennzeichens und Vergleich mit dem auf dem Protokoll ausgedruckten Echtheitskennzeichen durchgeführt wird.

7. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß zur Prüfung des Protokolls die Protokolldaten manuell in eine von der Sortiermaschine unabhängige Recheneinrichtung eingegeben werden und das von der Recheneinrichtung ermittelte und angezeigte Ergebnis mit dem auf dem Protokoll ausgedruckten Echtheitskennzeichen verglichen wird. 10
8. Verfahren nach Anspruch 6, dadurch **gekennzeichnet**, daß zur Prüfung des Protokolls die Daten über die Schnittstelle einer mit der Sortiervorrichtung verbundenen Einheit zugeführt werden, die automatisch anhand der Daten die Nachberechnung und den Vergleich durchführt. 15

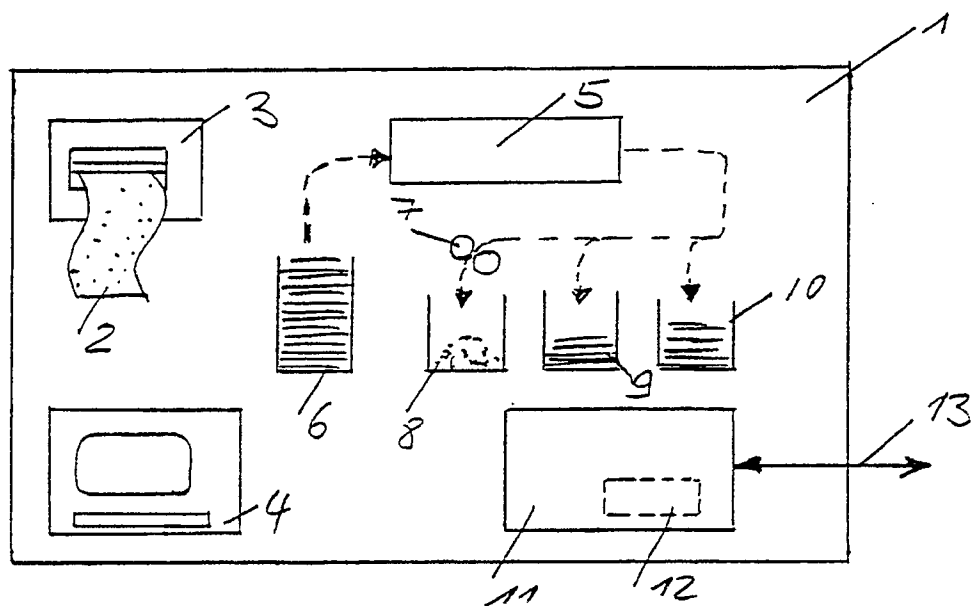


Fig. 1

Schichtprotokoll
Nr. 12.3

8 4 3 9 1

Datum 18.04.90
Zeit 16.43
Masch. Nr. 853
Bediener Nr. 635

U-BN 3000
Shr-3N 500
HN-BN 3

8 4 3 9 1

Fig. 2