(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 17 109 T2** 2004.04.29

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 901 060 B1**
(21) Deutsches Aktenzeichen: **698 17 109.8**
(96) Europäisches Aktenzeichen: **98 302 327.6**
(96) Europäischer Anmeldetag: **26.03.1998**
(97) Erstveröffentlichung durch das EPA: **10.03.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **13.08.2003**
(47) Veröffentlichungstag im Patentblatt: **29.04.2004**

(51) Int Cl.[7]: **G06F 1/00**

(30) Unionspriorität:
24140897 05.09.1997 JP

(84) Benannte Vertragsstaaten:
DE, GB

(73) Patentinhaber:
Fujitsu Ltd., Kawasaki, Kanagawa, JP

(74) Vertreter:
W. Seeger und Kollegen, 81369 München

(72) Erfinder:
Kashima, Kazunori, Tokyo, JP; Matsuura, Masataka, Nakahara-ku, Kanagawa 211, JP

(54) Bezeichnung: **Sichere Vorrichtung und Verfahren zur Datensteuerung**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein Geheimdatenverwaltungsgerät und -verfahren, das Geheimdaten wie z. B. einen geheimen Schlüssel steuert, den eine Zertifizierungsautorität für einen Benutzer vergibt. Die vorliegende Erfindung bezieht sich ferner auf ein computerlesbares Medium, das Programmcodeanweisungen speichert, die einen Prozessor veranlassen, eine Geheimdatenverwaltungsverarbeitung in einem Geheimdatenverwaltungsgerät auszuführen.

[0002] Allgemein wird in einem herkömmlichen Geheimdatenverwaltungssystem ein elektronisch gespeicherter geheimer Schlüssel gesteuert oder kontrolliert, indem ein mehrere alphanumerische Zeichen enthaltendes Paßwort verwendet wird, um eine Entdeckung durch einen Hacker zu vermeiden. Für einen Benutzer ist es erwünscht, mehrere verschiedene Paßworte zu verwenden, wenn er Zugang zu verschiedenen elektronischen Kommunikationsdiensten erlangt. Es ist jedoch praktisch schwierig für den Benutzer, sich an die jeweiligen Paßworte zum Erlangen solcher Dienste zu erinnern. In vielen Fällen verwendet der Benutzer ein einziges Paßwort, wenn er die Dienste in Anspruch nimmt.

[0003] In einem herkömmlichen System wird vom Benutzer oft ein auf persönlichen Informationen basierendes Paßwort wie z. B. ein Geburtsdatum oder eine Telefonnummer eingegeben. Die Möglichkeit, daß ein ernsthafter Hacker das auf persönliche Daten basierende Paßwort entdeckt ist, höher als eine mathematisch geschätzte Wahrscheinlichkeit der Entdeckung des Paßwortes.

[0004] Wenn der Benutzer des herkömmlichen Geheimdatenverwaltungssystems eine elektronische Kommunikation über das Internet vornimmt, gibt der Benutzer ferner oft ein alphanumerische Zeichen enthaltendes Paßwort ein. In solch einem Fall läuft der Benutzer Gefahr, das Paßwort an Hacker zu verlieren.

[0005] Wie oben beschrieben wurde, wird, wenn ein alphanumerische Zeichen enthaltendes Paßwort zum Steuern oder Kontrollieren des geheimen Schlüssels verwendet wird, die Möglichkeit der Entdeckung des Paßwortes gemäß der Art und Weise erhöht, in der der Benutzer das Paßwort verwendet.

[0006] Der durch die Verwendung des Paßwortes gesteuerte geheime Schlüssel gibt allgemein einen numerischen Wert mit mehreren hundert Ziffern an. Es ist praktisch unmöglich für den Benutzer, sich an den numerischen Wert des geheimen Schlüssels zu erinnern. In vielen Fällen wird ein Speichermedium wie z. B. eine IC-Karte verwendet, in der die Geheimdaten gespeichert sind. Wenn der geheime Schlüssel von der IC-Karte durch Verwenden des Paßwortes wie im obigen herkömmlichen System gesteuert wird, wird die Möglichkeit der Entdeckung des Paßwortes gemäß der Art und Weise erhöht, in der der Benutzer das Paßwort verwendet. Falls die IC-Karte von einem Hacker gestohlen wird, wird der Hacker das Paßwort leicht entdecken, um Zugang zu den Geheimdaten zu erlangen.

[0007] Wenn der geheime Schlüssel durch Verwenden des alphanumerischen Paßwortes im herkömmlichen Geheimdatenverwaltungssystem gesteuert wird, scheitert das herkömmliche System dabei, eine angemessene Sicherheit für die geheime Information im herkömmlichen System zu liefern.

[0008] Ein vorstellbares Verfahren, um die Sicherheit für die geheime Information im herkömmlichen System zu erhöhen, ist, ein alphanumerisches Paßwort zu verwenden, das eine große Anzahl Ziffern enthält, die schwer zu entdecken ist. Es ist jedoch für den Benutzer schwierig, sich an ein solches Paßwort zu erinnern, und der Gebrauch eines solchen Paßwortes ist für den Benutzer unbequem. Das oben erwähnte Verfahren scheitert auch dabei, angemessene Sicherheit für die geheime Information zu liefern.

[0009] Wie oben beschrieben wurde, gibt der Benutzer oft ein auf den Benutzer betreffenden persönlichen Daten basierendes Paßwort ein, wenn er Zugang zu der Geheiminformation erlangt. Die Möglichkeit, daß ein ernsthafter Hacker das auf den persönlichen Daten basierende Paßwort entdeckt, ist höher als die mathematisch geschätzte Wahrscheinlichkeit der Entdeckung des Paßwortes. Das herkömmliche Geheimdatenverwaltungssystem scheitert dabei, angemessene Sicherheit für die geheime Information zu liefern.

[0010] Wenn der Benutzer des herkömmlichen Geheimdatenverwaltungssystems ferner eine elektronische Kommunikation über das Internet vornimmt, muß der Benutzer ferner ein alphanumerische Zeichen enthaltendes Paßwort eingeben, indem statt einer Maus eine Tastatur eines Personalcomputers betätigt wird. Wenn er elektronische Kommunikationsdienste erlangt, betätigt im allgemeinen der Benutzer häufig die Maus. Der Benutzer muß die Tastatur nur betätigen, wenn er das Paßwort eingibt, und daher ist die Verwendung des alphanumerischen Paßwortes für den Benutzer erheblich unbequem.

[0011] Eine Aufgabe der vorliegenden Erfindung ist, ein verbessertes Geheimdatenverwaltungsgerät und Geheimdatenverwaltungsvenfahren zu schaffen, in denen die oben erwähnten Probleme eliminiert sind.

[0012] Eine andere Aufgabe der vorliegenden Erfindung ist, ein Geheimdatenverwaltungsgerät zu schaffen, welches ein einfaches Bildpaßwort nutzt, das durch Positionen von Eingabebildpunkten und eine Sequenz der Positionen erzeugt wird, die von einem Benutzer auf einem Anzeigemonitor unter Verwendung einer Eingabevorrichtung willkürlich spezifiziert werden, und angemessene Sicherheit für eine in einer Speichervorrichtung gespeicherte geheime Information liefert.

[0013] Noch eine weitere Aufgabe der vorliegenden Erfindung ist, ein Geheimdatenverwaltungsverfahren zu schaffen, welches ein einfaches Bildpaßwort nutzt, das durch Positionen von Eingabebildpunkten und eine Se-

quenz der Positionen erzeugt wird, die von einem Benutzer auf einem Anzeigemonitor unter Verwendung allein einer Eingabevorrichtung willkürlich spezifiziert werden, und angemessene Sicherheit für eine in einer Speichervorrichtung gespeicherte geheime Information liefert.

[0014] Eine weitere Aufgabe der vorliegenden Erfindung ist, ein computerlesbares Medium zu schaffen, das Programmcodeanweisungen speichert, um einen Prozessor eines Geheimdatenverwaltungsgeräts zu veranlassen, eine Geheimdatenverwaltungsverarbeitung auszuführen, die ein einfaches Bildpaßwort nutzt, das durch Positionen von Eingabebildpunkten und eine Sequenz der Positionen erzeugt wird, die von einem Benutzer auf einem Anzeigemonitor unter Verwendung einer Eingabevorrichtung willkürlich spezifiziert werden, und angemessene Sicherheit für eine in einer Speichervorrichtung gespeicherten geheimen Information liefert.

[0015] Gemäß einem ersten Gesichtspunkt der vorliegenden Erfindung wird ein Geheimdatenverwaltungsgerät zum Steuern eines geheimen Schlüssels geschaffen, so daß der geheime Schlüssel vertraulich gehalten wird, welches Geheimdatenverwaltungsgerät aufweist: eine Bildanzeigeeinheit, die ein Bild auf einem Anzeigemonitor anzeigt; eine Positions/Sequenzeingabeeinheit, die Positionen von Eingabebildpunkten auf dem unter Verwendung einer Eingabevorrichtung spezifizierten Bild eingibt und eine Sequenz der Positionen eingibt, die unter Verwendung der Eingabevorrichtung spezifiziert werden; eine Verschlüsselungseinheit, die verschlüsselte Daten des geheimen Schlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit erzeugt; eine Geheimdaten-Speichereinheit, die die verschlüsselten Daten des geheimen Schlüssels von der Verschlüsselungseinheit in einem Speichermedium speichert; eine Zugriffserlaubniseinheit, die einen Zugriff auf den geheimen Schlüssel erlaubt, der im Speichermedium gespeichert ist, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die unter Verwendung der Eingabeeinheit zu einer Zeit des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der Politions/Sequenzeingabeeinheit übereinstimmen; und eine Entschlüsselungseinheit, die Klardaten des geheimen Schlüssels aus den verschlüsselten Daten erzeugt, die im Speichermedium gespeichert sind, wenn der Zugriff durch die Zugriffserlaubniseinheit erlaubt wird.

[0016] Gemäß einem zweiten Gesichtspunkt der vorliegenden Erfindung wird ein Verfahren zum Steuern eines geheimen Schlüssels geschaffen, so daß der geheime Schlüssel vertraulich gehalten wird, welches Verfahren die folgenden Schritte aufweist: Eingeben von Benutzerdaten und Benutzerumgebungsdaten, die durch einen Benutzer spezifiziert werden; Festlegen eines auf einem Anzeigemonitor anzuzeigenden Bildes; Anzeigen des Bildes auf dem Anzeigemonitor und Eingeben von Positionen von Eingabebildpunkten auf dem angezeigten Bild, die durch den Benutzer spezifiziert werden, und einer Sequenz der Positionen, die durch den Benutzer spezifiziert wird; Erzeugen eines Verschlüsselungsschlüssels basierend auf den spezifizierten Positionen und der spezifizierten Sequenz; Erzeugen verschlüsselter Daten des geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel; und Speichern der verschlüsselten Daten des geheimen Schlüssels, der Benutzerdaten und der Benutzerumgebungsdaten in einem Speichermedium, worin die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten miteinander zusammenhängen und die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten im Speichermedium registriert sind.

[0017] Gemäß einem dritten Gesichtspunkt der vorliegenden Erfindung wird ein computerlesbares Medium geschaffen, das einen Programmcode speichert, um einen Prozessor zu veranlassen, eine Geheimdatenverwaltung auszuführen, welche einen geheimen Schlüssel steuert, der von einer Zertifizierungsautorität ausgegeben wurde, so daß der geheime Schlüssel in einem Geheimdatenverwaltungsgerät vertraulich gehalten wird, aufweisend: eine erste Programmcodevorrichtung, die den Prozessor veranlaßt, ein Bild auf einem Anzeigemonitor anzuzeigen; eine zweite Programmcodevorrichtung, die den Prozessor veranlaßt, Positionen von Eingabebildpunkten auf dem Bild, die unter Verwendung einer Eingabevorrichtung spezifiziert wurden, einzugeben und eine Sequenz der Positionen einzugeben, die unter Verwendung der Eingabevorrichtung spezifiziert wurde; eine dritte Programmcodevorrichtung, die den Prozessor veranlaßt, verschlüsselte Daten des geheimen Schlüssels basierend auf den Positionen und der Sequenz von der zweiten Programmcodevorrichtung zu erzeugen; eine vierte Programmcodevorrichtung, die den Prozessor veranlaßt, die verschlüsselten Daten des geheimen Schlüssels von der dritten Programmcodevorrichtung in einem ersten Speichermedium zu speichern; eine fünfte Programmcodevorrichtung, die den Prozessor veranlaßt, einen Zugriff auf den im ersten Speichermedium gespeicherten geheimen Schlüssel zu erlauben, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die unter Verwendung der Eingabevorrichtung zu einem Zeitpunkt des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der zweiten Programmcodevorrichtung übereinstimmen; und eine sechste Programmcodevorrichtung, die den Prozessor veranlaßt, Klardaten des geheimen Schlüssels aus den im ersten Speichermedium gespeicherten verschlüsselten Daten zu erzeugen, wenn der Zugriff erlaubt wird.

[0018] In dem Geheimdatenverwaltungsgerät und -verfahren der vorliegenden Erfindung wird der Verschlüsselungsschlüssel durch Positionen von Eingabebildpunkten und eine Sequenz der Positionen erzeugt, die von einem Benutzer auf dem Anzeigemonitor unter Verwendung allein der Eingabevorrichtung spezifiziert werden, und wird der geheime Schlüssel durch Verwenden des Verschlüsselungsschlüssels gesteuert oder kontrolliert. Es ist nicht länger notwendig, das alphanumerische Paßwort durch Verwenden der Tastatur wie im herkömm-

lichen System einzugeben. Es ist möglich, daß die vorliegende Erfindung eine erhöhte Bedienbarkeit für den Benutzer und angemessene Sicherheit für die geheime Information im Speichermedium liefert.

[0019] Gemäß der vorliegenden Erfindung ist es nicht notwendig, das Personaldaten-Paßwort wie z. B. ein Geburtsdatum oder eine Telefonnummer zu verwenden. Die Positionen der Eingabebildpunkte und die Sequenz der Positionen werden durch den Benutzer auf dem Anzeigemonitor unter Verwendung der Eingabevorrichtung willkürlich spezifiziert und beziehen sich nicht auf persönliche Daten. Es ist möglich, daß die vorliegende Erfindung angemessene Sicherheit für die Geheiminformation liefert, und das Geheimdatenverwaltungsgerät und -verfahren der vorliegenden Erfindung sind beim Vermeiden der Entdeckung des Paßwortes durch einen Hacker effektiv.

[0020] Wenn der Benutzer des Geheimdatenverwaltungsgerätes der vorliegenden Erfindung eine elektronische Kommunikation über das Internet vornimmt, ist es ferner nicht notwendig, daß der Benutzer die Tastatur des Computers während der Kommunikation betätigt. Die Positionen der Eingabebildpunkte und die Sequenz der Positionen können durch den Benutzer auf dem Anzeigemonitor unter Verwendung allein der Eingabevorrichtung spezifiziert werden, und es ist möglich, daß die vorliegende Erfindung eine erhöhte Bedienbarkeit für den Benutzer und angemessene Sicherheit für die Geheiminformation liefert.

[0021] Das Geheimdatenverwaltungsgerät und -verfahren der vorliegenden Erfindung erfordert ferner keine teure Hardware wie z. B. ein Fingerabdrucksystem oder ein Sprachmustersystem, um eine persönliche Identifizierung zu authentifizieren, und kann allein durch Implementieren von Software konstruiert werden.

[0022] Die obigen und andere Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden aus der folgenden ausführlichen Beschreibung ersichtlicher werden, wenn sie in Verbindung mit den beiliegenden Zeichnungen gelesen wird, in denen:

[0023] **Fig.** 1 ein Blockdiagramm von Basiselementen eines Geheimdatenverwaltungsgerätes der vorliegenden Erfindung ist;

[0024] **Fig.** 2 ein Blockdiagramm des Geheimdatenverwaltungsgerätes der vorliegenden Erfindung ist;

[0025] **Fig.** 3 ein Flußdiagramm zum Erläutern einer Verarbeitung eines Eintrags eines geheimen Schlüssels eines Geheimdatenverwaltungsverfahrens der vorliegenden Erfindung ist;

[0026] **Fig.** 4 ein Flußdiagramm zum Erläutern einer Benutzerauthentifizierungsverarbeitung des Geheimdatenverwaltungsverfahrens der vorliegenden Erfindung ist;

[0027] **Fig.** 5 ein Blockdiagramm zum Erläutern einer bevorzugten Ausführungsform des Geheimdatenverwaltungsgeräts der vorliegenden Erfindung ist;

[0028] **Fig.** 6 ein Flußdiagramm zum Erläutern einer Neueintrag-Verarbeitung ist, die vom Geheimdatenverwaltungsgerät von **Fig.** 5 durchgeführt wird;

[0029] **Fig.** 7A und **Fig.** 7B Diagramme zum Erläutern der Inhalte einer Datenbank für geheime Schlüssel und einer Datenbank für Festlegungen von Benutzerumgebungen in dem Geheimdatenverwaltungsgerät von **Fig.** 5 sind;

[0030] **Fig.** 8 ein Flußdiagramm zum Erläutern einer Bildpaßwortverarbeitung ist, die von dem Geheimdatenverwaltungsgerät von **Fig.** 5 durchgeführt wird;

[0031] **Fig.** 9 ein Flußdiagramm zum Erläutern einer Zusatzeintrag-Verarbeitung ist, die vom Geheimdatenverwaltungsgerät von **Fig.** 5 durchgeführt wird;

[0032] **Fig.** 10 ein Diagramm zum Erläutern der Inhalte der Datenbank für geheime Schlüssel ist, nachdem die Zusatzeintrag-Verarbeitung durchgeführt ist;

[0033] **Fig.** 11 ein Flußdiagramm zum Erläutern einer Eintrag-Aktualisierungsverarbeitung ist, die vom Geheimdatenverwaltungsgerät von **Fig.** 5 durchgeführt wird;

[0034] **Fig.** 12 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Benutzerumgebungen festlegenden Schritt ist;

[0035] **Fig.** 13 ein Diagramm zum Erläutern eines Anzeigeschirnis des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Hintergrundbilder festlegenden Schritt ist;

[0036] **Fig.** 14 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Maschenmuster festlegenden Schritt ist;

[0037] **Fig.** 15 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Positions/Sequenzdaten festlegenden Schritt ist;

[0038] **Fig.** 16 ein Diagramm zum Erläutern einer Konfiguration einer Verschlüsselungsschlüssel erzeugenden Einheit im Geheimdatenverwaltungsgerät von **Fig.** 5 ist;

[0039] **Fig.** 17 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Verschlüsselungsschlüssel erzeugenden Schritt ist;

[0040] **Fig.** 18 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem einen geheimen Schlüssel festlegenden Schritt ist;

[0041] **Fig.** 19 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem registrierte Benutzernamen festlegenden Schritt ist;

[0042] **Fig.** 20 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von

Fig. 5 bei einem Hintergrund/Musteranzeigeschritt ist;

[0043] **Fig.** 21 ein Diagramm zum Erläutern eines Anzeigeschirms des Geheimdatenverwaltungsgeräts von **Fig.** 5 bei einem Bildpaßwort-Empfangsschritt ist; und

[0044] **Fig.** 22A und **Fig.** 22B Diagramme zum Erläutern von Anzeigeschirmen eines Browsers sind, wenn eine Browser-Link-Option verwendet wird.

[0045] Um das Verständnis der vorliegenden Erfindung zu erleichtern, werden die Prinzipien eines Geheimdatenverwaltungsgeräts und -verfahrens der vorliegenden Erfindung mit Verweis auf **Fig.** 1 bis **Fig.** 4 beschrieben.

[0046] **Fig.** 1 zeigt Basiselemente eines Geheimdatenverwaftungsgeräts der vorliegenden Erfindung, in welchem ein geheimer Schlüssel so gesteuert wird, daß der geheime Schlüssel vertraulich gehalten wird.

[0047] Wie in **Fig.** 1 dargestellt ist, umfaßt ein Geheimdatenverwaltungsgerät **2** eine Bildanzeigeeinheit **10**, die ein Bild auf einem Anzeigemonitor **4** anzeigt. Eine Positions/Sequenzeingabeeinheit **12** gibt Positionen von Bildeingabepunkten auf dem Bild ein, die von einem Benutzer durch Verwenden einer Maus **6** spezifiziert werden, und gibt eine durch Verwenden der Maus **6** spezifizierte Sequenz der Positionen ein. Die Maus **6** in dem Geheimdatenverwaltungsgerät **2** kann irgendeine von Eingabevorrichtungen einschließlich einer Zeigervorrichtung, eines Trackball, eines Joystick usw. sein. Eine Verschlüsselungseinheit **14** erzeugt verschlüsselte Daten eines geheimen Schlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **12**. Eine Geheimdaten-Speichereinheit **16** speichert die verschlüsselten Daten des geheimen Schlüssels von der Verschlüsselungseinheit **14** in einem (in **Fig.** 1 nicht dargestellten) Speichermedium.

[0048] In dem Geheimdatenverwaltungsgerät **2** erlaubt ferner eine Zugriffserlaubniseinheit **18** einen Zugriff auf den geheimen Schlüssel im Speichermedium, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die durch den Benutzer unter Verwendung einer Maus zu einem Zeitpunkt eines Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **12** übereinstimmen. Eine Entschlüsselungseinheit **20** erzeugt Klardaten des geheimen Schlüssels aus den verschlüsselten Daten, die im Speichermedium gespeichert sind, wenn durch die Zugriffserlaubniseinheit **18** ein Zugriff erlaubt wird.

[0049] In dem oben beschriebenen Geheimdatenverwaltungsgerät **2** wird ein Zugriff auf den geheimen Schlüssel im Speichermedium gesteuert, indem die Positionen und die Sequenz auf dem Bild genutzt werden, die vom Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** spezifiziert wurden. Der Zugriff auf den geheimen Schlüssel wird nur erlaubt, wenn die nachfolgenden spezifizierten Positionen und die Sequenz (oder das Bildpaßwort) mit den ursprünglich spezifizierten Positionen und der Sequenz (oder dem Bildpaßwort) übereinstimmen. Da das Bildpaßwort durch den Benutzer beliebig spezifiziert werden kann und nicht wie im herkömmlichen System auf persönlichen Daten beruht, kann das Geheimdatenverwaltungsgerät gemäß der vorliegenden Erfindung eine erhöhte Bedienbarkeit für den Benutzer und eine angemessene Sicherheit für den geheimen Schlüssel im Speichermedium liefern. Es ist möglich, daß das Geheimdatenverwaltungsgerät der vorliegenden Erfindung die Möglichkeit merklich reduziert, daß ein Hacker das Bildpaßwort entdecken wird, verglichen mit dem Fall eines alphanumerischen Paßwortes des herkömmlichen Systems.

[0050] In dem Geheimdatenverwaltungsgerät **2** von **Fig.** 1 kann die Verschlüsselungseinheit **14** eine Verschlüsselungsschlüssel erzeugende Einheit enthalten, die basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **12** einen Verschlüsselungsschlüssel erzeugt, und eine Geheimschlüssel-Verschlüsselungseinheit, die verschlüsselte Daten des geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel von der Verschlüsselungsschlüssel erzeugenden Einheit erzeugt.

[0051] In dem oben beschriebenen Geheimdatenverwaltungsgerät **2** wird der geheime Schlüssel gesteuert durch Verwenden eines Verschlüsselungsschlüssels, der durch die Positionen der Eingabebildpunkte und die Sequenz der Positionen, die durch den Benutzer spezifiziert wurden, erzeugt wird, und die verschlüsselten Daten des geheimen Schlüssels werden im Speichermedium gespeichert. Das Geheimdatenverwaltungsgerät der vorliegenden Erfindung kann eine höhere Sicherheit für die Geheiminformation liefern als das herkömmliche System, in welchem der Klartext des geheimen Schlüssels im Speichermedium gespeichert ist.

[0052] Ferner kann in der Verschlüsselungseinheit **14** des Geheimdatenverwaltungsgeräts **2** von **Fig.** 1 die Verschlüsselungsschlüssel erzeugende Einheit einen Wert des Verschlüsselungsschlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **12** berechnen. Die Geheimschlüssel-Verschlüsselungseinheit kann eine Eins-zu-Eins-Buchstabensubstitution eines eingegebenen geheimen Schlüssels gemäß dem berechneten Wert von der Verschlüsselungsschlüssel erzeugenden Einheit durchführen.

[0053] Das oben beschriebene Geheimdatenverwaltungsgerät **2** kann die Möglichkeit merklich reduzieren, daß ein Hacker das Bildpaßwort entdeckt, verglichen mit dem Fall des alphanumerischen Paßwortes wie im herkömmlichen System.

[0054] Ferner kann in dem Geheimdatenverwaltungsgerät **2** von **Fig.** 2 die Bildanzeigeeinheit **10** ein Maschenmuster anzeigen, das auf dem Bild auf dem Anzeigemonitor überlagert wird, welches Maschenmuster eine auswählbare Maschengröße und eine auswählbare Maschenmusterform hat. Das oben beschriebene Ge-

heimdatenverwaltungsgerät **2** kann eine erhöhte Bedienbarkeit für den Benutzer liefern, wenn die Positionen der Eingabebildpunkte und die Sequenz der Positionen auf dem Bild auf dem Anzeigemonitor spezifiziert werden.

[0055] **Fig.** 2 zeigt eine Konfiguration des Geheimdatenverwaltungsgeräts der vorliegenden Erfindung. In dem Geheimdatenverwaltungsgerät von **Fig.** 2 wird ein von einer Zertifizierungsautorität ausgegebener geheimer Schlüssel so gesteuert, daß der geheime Schlüssel vertraulich gehalten wird.

[0056] In **Fig.** 2 sind die Elemente, welche die gleichen wie entsprechende Elemente in **Fig.** 1 sind, durch die gleichen Bezugsziffern bezeichnet, und deren Beschreibung wird weggelassen.

[0057] Wie in **Fig.** 2 gezeigt ist, umfaßt ein Geheimdatenverwaltungsgerät **30** eine Bildanzeigeeinheit **32**, die ein Bild auf dem Anzeigemonitor **4** anzeigt. Eine Positions/Sequenzeingabeeinheit **40** gibt Positionen von Eingabebildpunkten auf dem Bild ein, die von einem Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** spezifiziert wurden, und gibt eine Sequenz der Positionen ein, die vom Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** spezifiziert wurde. Eine Verschlüsselungseinheit **42** erzeugt verschlüsselte Daten des geheimen Schlüssels von der Zertifizierungsautorität basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **40**. Eine Geheimdaten-Speichereinheit **50** speichert die verschlüsselten Daten des geheimen Schlüssels von der Verschlüsselungseinheit **42** in einem (nicht dargestellten) Speichermedium.

[0058] In dem Geheimdatenverwaltungsgerät **30** von **Fig.** 2 erlaubt ferner eine Zugriffserlaubniseinheit **60** einen Zugriff auf den im Speichermedium gespeicherten geheimen Schlüssel, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die vom Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** zur Zeit des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **40** übereinstimmen. Eine Entschlüsselungseinheit **66** erzeugt Klardaten des geheimen Schlüssels aus den im Speichermedium gespeicherten verschlüsselten Daten, wenn der Zugriff durch die Zugriffserlaubniseinheit **60** erlaubt wird.

[0059] Im Geheimdatenverwaltungsgerät **30** von **Fig.** 2 umfaßt die Verschlüsselungseinheit **42** eine Verschlüsselungsschlüssel erzeugende Einheit **44**, die basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **40** einen Verschlüsselungsschlüssel erzeugt, und eine Geheimschlüssel-Verschlüsselungseinheit **46**, die verschlüsselte Daten des geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel von der Verschlüsselungsschlüssel erzeugenden Einheit **44** erzeugt.

[0060] In der oben beschriebenen Verschlüsselungseinheit **42** des Geheimdatenverwaltungsgeräts **30** berechnet die Verschlüsselungsschlüssel erzeugende Einheit **44** einen Wert des Verschlüsselungsschlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **40**. Die Geheimschlüssel-Verschlüsselungseinheit **46** führt eine Eins-zu-Eins-Buchstabensubstitution des geheimen Schlüssels von der Zertifizierungsautorität gemäß dem berechneten Wert von der Verschlüsselungsschlüssel erzeugenden Einheit **44** durch.

[0061] In dem Geheimdatenverwaltungsgerät **30** von **Fig.** 2 zeigt die Bildanzeigeeinheit **32** ein registriertes Bild **34** auf dem Anzeigemonitor **4** an. Im oben beschriebenen Geheimdatenverwaltungsgerät **30** kann die Bildanzeigeeinheit **32** ein benutzerdefiniertes Bild **36** auf dem Anzeigemonitor **4** anzeigen. In dem oben beschriebenen Geheimdatenverwaltungsgerät **30** kann ferner die Bildanzeigeeinheit **32** ein von einem separaten Speichermedium übertragenes benutzerdefiniertes Bild auf dem Anzeigemonitor **4** anzeigen. Dieses Speichermedium ist von dem Speichermedium innerhalb des Geheimdatenverwaltungsgeräts **30** getrennt. Dies ermöglicht dem Geheimdatenverwaltungsgerät der vorliegenden Erfindung, eine erhöhte Sicherheit für das vom Benutzer spezifizierte Bildpaßwort zu liefern.

[0062] Das Geheimdatenverwaltungsgerät **30** von **Fig.** 2 umfaßt ferner eine Maschenmusteranzeigeeinheit **38**, die ein auf dem Bild auf dem Anzeigemonitor **4** überlagertes Maschenmuster anzeigt, welches Maschenmuster eine auswählbare Maschengröße und eine auswählbare Maschenmusterfarbe aufweist.

[0063] In dem Geheimdatenverwaltungsgerät **30** von **Fig.** 2 kann die Verschlüsselungseinheit **42** verschlüsselte Daten mehrerer geheimer Schlüssel erzeugen, wenn identische Positionen von Eingabebildpunkten auf dem Bild und eine identische Sequenz der Positionen vom Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** spezifiziert und durch die Positions/Sequenzeingabeeinheit 40 eingegeben werden. In diesem Fall kann die Zugriffserlaubniseinheit **60** einen Zugriff auf die mehreren Schlüssel erlauben, wenn die identischen Positionen und die identische Sequenz vom Benutzer auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** zu einem Zeitpunkt des Zugriffs nachfolgend spezifiziert werden. In diesem Fall kann, wenn der Benutzer zu der Zeit eines Zugriffs auf die mehreren geheimen Schlüssel die identischen Positionen und die identische Sequenz auf dem Anzeigemonitor **4** durch Verwenden der Maus **6** spezifiziert, die Zugriffserlaubniseinheit **60** den Zugriff auf die mehreren geheimen Schlüssel erlauben.

[0064] Das Geheimdatenverwaltungsgerät **30** von **Fig.** 2 umfaßt ferner eine zweite Eingabeeinheit **68**, die Benutzerdaten und Benutrerumgebungsdaten eingibt, die vom Benutzer spezifiziert wurden. Wie in **Fig.** 2 gezeigt ist, speichert die Geheimdaten-Speichereinheit **50** die Benutzerdaten **54** und die Benutrerumgebungsdaten **56** im Speichermedium zusätzlich zu den verschlüsselten Daten **52** des geheimen Schlüssels.

[0065] In dem oben beschriebenen Geheimdatenverwaltungsgerät **30** umfaßt die Zugriffserlaubniseinheit **60** eine Zugriffsmöglichkeit-Beurteilungseinheit **62**, die bestimmt, ob Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die vom Benutzer auf den Anzeigemonitor **4** durch Verwenden der Maus **6** zu einer Zeit des Zugriffs spezifiziert werden, mit den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit **40** übereinstimmen, und eine Geheimschlüssel-Auswahleinheit **64**, die zusätzlich zu den verschlüsselten Daten **52** des geheimen Schlüssels die Benutzerdaten **54** und die Benutzerumgebungsdaten **56** aus dem Speichermedium ausliest, wenn der Zugriff auf den geheimen Schlüssel von der Zugriffserlaubniseinheit **60** erlaubt wird. Dies ermöglicht dem Geheimdatenverwaltungsgerät der vorliegenden Erfindung, eine erhöhte Bedienbarkeit für den Benutzer zu liefern.

[0066] **Fig.** 3 zeigt eine Geheimschlüssel-Eintragverarbeitung eines Geheimdatenverwaltungsverfahrens der vorliegenden Endung. In dem Geheimdatenverwaltungsverfahren von **Fig.** 3 wird ein von einer Zertifizierungsautorität ausgegebener geheimer Schlüssel durch Verwenden eines Verschlüsselungsschlüssels gesteuert, der durch Positionen von Eingabebildpunkten und eine Sequenz der Positionen erzeugt wurde, die von einem Benutzer spezifiziert wurden, so daß der geheime Schlüssel vertraulich gehalten wird.

[0067] Das Geheimdatenverwaltungsverfahren von **Fig.** 3 bezieht sich auf eine Geheimschlüssel-Eintragverarbeitung. Wie in **Fig.** 3 gezeigt ist, werden am Beginn der Geheimschlüssel-Eintragsverarbeitung des Geheimdatenverwaltungsverfahrens der vorliegenden Erfindung Benutzerdaten und Benutzerumgebungsdaten, die von einem Benutzer spezifiziert werden, in das Geheimdatenverwaltungsgerät eingegeben (S1). Ein auf dem Anzeigemonitor anzuzeigendes Bild wird durch den Benutzer spezifiziert (S2). Das Bild wird auf dem Anzeigemonitor angezeigt, und Positionen von Eingabebildpunkten des Bildes auf dem Anzeigemonitor, die durch Verwenden der Maus vom Benutzer spezifiziert werden, und eine Sequenz der Positionen, die vom Benutzer spezifiziert wird, werden in das Geheimdatenverwaltungsgerät eingegeben (S3).

[0068] Ferner wird in der Geheimschlüssel-Eintragsverarbeitung ein Verschlüsselungsschlüssel basierend auf den spezifizierten Positionen und der spezifizierten Sequenz erzeugt (S4). Verschlüsselte Daten des geheimen Schlüssels werden basierend auf dem Verschlüsselungsschlüssel erzeugt (S5). Die verschlüsselten Daten des geheimen Schlüssels, die Benutzerdaten und die Benutzerumgebungsdaten werden in einem Speichermedium des Geheimdatenverwaltungsgeräts gespeichert (S6). Im Speichermedium sind die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten aufeinander bezogen, und die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten sind im Speichermedium registriert (S6).

[0069] **Fig.** 4 zeigt eine Benutzerauthentifizierungs-Verarbeitung des Geheimdatenverwaltungsverfahrens der vorliegenden Erfindung. In dem Geheimdatenverwaltungsverfahren von **Fig.** 4 wird ein Zugriff auf den von der Zertifizierungsautorität ausgegebenen geheimen Schlüssel gesteuert durch Durchführen einer Benutzerauthentifizierung, nachdem die Geheimschlüssel-Eintragverarbeitung von **Fig.** 3 beendet ist.

[0070] Wie in **Fig.** 4 gezeigt ist, werden am Beginn der Benutzerauthentifizierungs-Verarbeitung des Geheimdatenverwaltungsverfahrens der vorliegenden Erfindung die Benutzerdaten, die durch den Benutzer zu einem Zeitpunkt eines Zugriffs nachfolgend spezifiziert werden, in das Geheimdatenverwaltungsgerät eingegeben (S7). Das Bild wird auf dem Anzeigemonitor angezeigt, und Positionen von Eingabebildpunkten auf dem Bild auf dem Anzeigemonitor, die vom Benutzer nachfolgend spezifiziert werden, und eine Sequenz der Positionen, die vom Benutzer nachfolgend spezifiziert wird, werden in das Geheimdatenverwaltungsgerät eingegeben (S8).

[0071] Nachdem der obige Schritt S8 durchgeführt ist, wird eine Entscheidung diesbezüglich getroffen, ob die nachfolgend spezifizierten Positionen und Sequenz des Bildpaßwortes mit den vorher spezifizierten Positionen und der Sequenz des Bildpaßwortes übereinstimmen (S9).

[0072] Wenn der obige Bestimmungsschritt S9 die Übereinstimmung ergibt, werden Klardaten des auf den Benutzernamen bezogenen geheimen Schlüssels aus den im Speichermedium gespeicherten verschlüsselten Daten erzeugt, und ein Zugriff auf den geheimen Schlüssel wird gemäß den auf den geheimen Schlüssel bezogenen Benutzerumgebungsdaten erlaubt (S11).

[0073] Wenn auf der anderen Seite der obige Bestimmungsschritt S9 keine Übereinstimmung ergibt, wird der Zugriff auf den geheimen Schlüssel gesperrt (S10). Demgemäß kann das Geheimdatenverwaltungsverfahren der vorliegenden Erfindung eine erhöhte Bedienbarkeit für den Benutzer und eine angemessene Sicherheit für die Geheiminformation liefern.

[0074] Im Hinblick auf das oben beschriebene Geheimdatenverwaltungsgerät und -verfahren wird nun die bevorzugte Ausführungsform des Geheimdatenverwaltungsgeräts der vorliegenden Erfindung mit Verweis auf **Fig.** 5 bis **Fig.** 22B beschrieben.

[0075] **Fig.** 5 zeigt eine Ausführungsform des Geheimdatenverwaltungsgeräts der vorliegenden Erfindung.

[0076] In einem Geheimdatenverwaltungssystem **100** der vorliegenden Ausführungsform wird ein geheimer Schlüssel, um Zugriff auf in einem Speichermedium gespeicherte geheime Informationen zu erhalten, erzeugt, indem ein Verschlüsselungsschlüssel verwendet wird, der durch Positionen von Eingabebildpunkten und eine Sequenz der Positionen erzeugt wurde. Die Positionen der Eingabebildpunkte und die Sequenz der Positionen werden durch den Bildpaßwortbenutzer auf dem Anzeigemonitor mit der Maus willkürlich spezifiziert. Das Ge-

heimdatenverwaltungssystem **100** steuert einen Zugriff auf die geheime Information, indem eine Bestimmung diesbezüglich durchgeführt wird, ob ein für den Zugriff vergegebenes eingegebenes Bildpaßwort mit einem registrierten Bildpaßwort (oder den Positionen der Eingabebildpunkte und der Sequenz der Position) übereinstimmt, das innerhalb des Systems **100** gespeichert ist.

[0077] Wie in **Fig.** 5 gezeigt ist, umfaßt das Geheimdatenverwaltungssystem **100** eine Verarbeitungssteuereinheit **102**. Als Antwort auf einen eingegebenen Befehl wählt die Verarbeitungssteuereinheit **102** eine von mehreren Verarbeitungseinheiten innerhalb des Geheimdatenverwaltungssystems **100** aus und führt eine entsprechende Verarbeitung für die ausgewählte der mehreren Verarbeitungseinheiten durch. Die mehreren Verarbeitungseinheiten schließen eine Neueintrag-Verarbeitungseinheit **103**, eine Bildpaßwort-Verarbeitungseinheit **104**, eine Zusatzeintrag-Verarbeitungseinheit **105** und eine Eintragaktualisierungs-Verarbeitungseinheit **106** ein.

[0078] In dem Geheimdatenverwaltungssystem **100** von **Fig.** 5 sind ferner Geheimschlüsseldatenbank **131** und eine Benutzerumgebungsdatenbank **132** vorgesehen. In der Geheimschlüsseldatenbank **131** sind mehrere Geheimschlüsseldaten gespeichert. In der Benutzerumgebungsdatenbank **132** sind mehrere Benutzerumgebungen festlegende Daten gespeichert.

[0079] In der Neueintrag-Verarbeitungseinheit **103** des Systems **100** von **Fig.** 5 sind eine Benutzerumgebungen festlegende Einheit **111**, eine Hintergrundbilder festlegende Einheit **112**, eine Maschenmuster festlegende Einheit **113**, eine Positions/Sequenzdaten festlegende Einheit **114**, eine Verschlüsselungsschlüssel erzeugende Einheit **115**, eine Geheimschlüssel festlegende Einheit **116**, eine Verschlüsselungseinheit **117**, eine Geheimschlüssel speichernde Einheit **118** und eine Festlegungen von Benutzerumgebungen speichernde Einheit **119** vorgesehen.

[0080] **Fig.** 6 zeigt eine Neueintrag-Verarbeitung, die durch die Neueintrag-Verarbeitungseinheit **103** in dem Geheimdatenverwaltungssystem **100** durchgeführt wird.

[0081] In der vorliegenden Ausführungsform ist ein Neueintrag-Verarbeitungsprogramm, das auf das Flußdiagramm von **Fig.** 6 bezogen ist (was später beschrieben wird), Programmcodeanweisungen, die in einem (nicht dargestellten) Speicher des Geheimdatenverwaltungssystems **100** gespeichert sind. Der Speicher des Geheimdatenverwaltungssystems **100** ist z. B. ein ROM (Nurlesespeicher) oder einen RAM (Direktzugriffsspeicher). Der Speicher entspricht in den Ansprüchen einem computerlesbaren Medium. Das computerlesbare Medium umfaßt eine beliebige Anweisungsspeichervorrichtung wie z. B. Magnetplatten, die Disketten einschließen, optische oder Bildplatten, die CD-ROMs einschließen, magnetooptische Platten einschließlich MOs, Halbleiterspeicherkarten wie IC-Karten und Miniaturkarten und andere Arten von von computernutzbaren Vorrichtungen und Medien.

[0082] In der vorliegenden Ausführungsform kann der Speicher des Geheimdatenverwaltungssystems **100** codierte oder nicht codierte Anweisungen speichern. Die Anweisungen können zuerst von einer Diskette (oder einem CD-ROM) auf ein (nicht dargestelltes) Festplattenlaufwerk des Geheimdatenverwaltungssystems **100** installiert, zu einem (nicht dargestellten) RAM des Systems **100** übertragen und dann von einem (nicht dargestellten) Prozessor des Systems **100** gelesen werden. Der Speicher des Geheimdatenverwaltungssystems **100** kann entweder alle oder einen Teil der auf das Flußdiagramm von **Fig.** 6 bezogenen Anweisungen speichern.

[0083] In der vorliegenden Ausführungsform enthält ferner die Verarbeitungssteuereinheit **102** einen Prozessor (z. B. eine zentrale Verarbeitungseinheit des Geheimdatenverwaltungssystems **100**). Die oben erwähnten Programmcodeanweisungen veranlassen den Prozessor der Verarbeitungssteuereinheit **102**, eine entsprechende Verarbeitung für die ausgewählte der Verarbeitungseinheiten **103**–**106** durchzuführen. Im folgenden wird der Prozessor der Verarbeitungssteuereinheit **102** des Geheimdatenverwaltungssystems **100** der einfachen Beschreibung halber einfach der Prozessor genannt.

[0084] Während der Neueintrag-Verarbeitung von **Fig.** 6 werden vom Bildpaßwort-Benutzer ein Geheimschlüsseleintrag in der Geheimschlüsseldatenbank **131** und ein Benutzerumgebungen festlegender Eintrag, der sich auf den Geheimschlüsseleintrag bezieht, in der Benutzerumgebungen festlegenden Datenbank **132** ausgeführt.

[0085] Am Beginn der Neueintrag-Verarbeitung von **Fig.** 6 veranlaßt die Benutzerumgebungen festlegende Einheit **111** bei Schritt S21 den Prozessor, eine Festlegung von Benutzerumgebungen für das Geheimdatenverwaltungssystem **100** zu empfangen, die vom Benutzer auf dem Anzeigemonitor unter Verwendung der Maus eingegeben wird. Die Eingabe einer Umgebungsfestlegung durch den Benutzer beinhaltet einen Benutzernamen, einen benutzten Browser und eine Browser-Link-Option. Die eingegebene Umgebungsfestlegung für das System **100** wird während der nachfolgenden Verarbeitung der Neueintrag-Verarbeitungseinheit **103** verwendet, um eine erhöhte Bedienbarkeit für den Benutzer zu liefern.

[0086] Falls beim obigen Schritt S21 als der Benutzername der Umgebungsfestlegung ein registrierter Benutzername eingegeben wird, kann der registrierte Benutzername während einer nachfolgenden Verarbeitung der Neueintrag-Verarbeitungseinheit **103** verwendet werden. Der registrierte Benutzername kann beliebige Identifizierungsdaten umfassen, um den Benutzer zu identifizieren, und er muß nicht notwendigerweise der wirkli-

che Name des Benutzers sein. Es ist notwendig, daß die Identifizierungsdaten dem Hacker nicht einfach ermöglichen, den Benutzer zu erkennen.

[0087] Die Umgebungsfestlegung für das System **100** wird vom Benutzer beim obigen Schritt S21 willkürlich eingegeben, und es ist möglich, eine erhöhte Bedienbarkeit der Maus für den Benutzer während der nachfolgenden Verarbeitung der Neueintrag-Verarbeitungseinheit zu schaffen.

[0088] Nachdem der obige Schritt S21 durchgeführt ist, veranlaßt die Hintergrundbilder festlegende Einheit **112** bei Schritt S22 den Prozessor, ein vom Benutzer eingegebenes Hintergrundbild zu empfangen. Das eingegebene Hintergrundbild wird auf dem Anzeigemonitor angezeigt, nachdem der obige Schritt S22 während der Neueintrag-Verarbeitung ausgeführt ist.

[0089] Beim obigen Schritt S22 wählt der Benutzer als das eingegebene Hintergrundbild von mehreren registrierten Hintergrundbildern, einem benutrerdefinierten Hintergrundbild oder einem anderen, von einem externen Bildspeichermedium in das System **100** übertragenen Hintergrundbild aus. Das Bildspeichermedium umfaßt irgendeine Bildspeichervorrichtung wie z. B. Magnetplatten einschließlich Disketten, optische Platten einschließlich CD-ROMS, magnetooptische Platten einschließlich MOs, Halbleiterspeicherkarten und andere Arten von computernutzbaren Vorrichtungen und Medien.

[0090] Nachdem der obige Schritt S22 durchgeführt ist, veranlaßt die Maschenmuster festlegende Einheit **113** bei Schritt S23 den Prozessor, ein vom Benutzer eingegebenes Maschenmuster zu empfangen. Das eingegebene Maschenmuster wird auf dem Hintergrundbild auf dem Anzeigemonitor während der nachfolgenden Verarbeitung der Neueintrag-Verarbeitungseinheit **103** überlagert.

[0091] Positionen eingegebener Bildpunkte, die vom Benutzer auf dem Anzeigemonitor mit der Maus während der Bildpaßwortverarbeitung spezifiziert wurden, können nicht empfindlich genug sein, damit das System **100** sie erkennt. Das auf dem Hintergrundbild überlagerte Maschenmuster ermöglicht dem System **100**, die jeweiligen Bildpunkte von Eingabebildpunkten, die vom Benutzer spezifiziert werden, mit erhöhter Genauigkeit zu erkennen.

[0092] Nachdem der obige Schritt S23 durchgeführt ist, veranlaßt die Positions/Sequenzdaten festlegende Einheit **114** bei Schritt S24 den Prozessor, Positionen von Eingabebildpunkten und eine Sequenz der Positionen zu empfangen, die vom Benutzer auf dem Anzeigemonitor mit der Maus spezifiziert wurden. Wie oben beschrieben wurde, wird das Hintergrundbild, auf dem das Maschenmuster überlagert ist, auf dem Anzeigemonitor angezeigt, und der Benutzer spezifiziert die Positionen von Eingabebildpunkten auf dem Hintergrundbild durch Verwenden der Maus. Die Anzahl der Eingabebildpunkte, die vom Benutzer spezifiziert wurden, entspricht der Anzahl Ziffern des Bildpaßwortes.

[0093] Nachdem der obige Schritt S24 durchgeführt ist, veranlaßt die Verschlüsselungsschlüssel erzeugende Einheit **115** bei Schritt S25 den Prozessor, basierend auf den spezifizierten Positionen der Eingabebildpunkte und der spezifizierten Sequenz der Positionen, die beim obigen Schritt S24 erhalten wurden, einen Verschlüsselungsschlüssel zu erzeugen. Der beim obigen Schritt S25 erhaltene Verschlüsselungsschlüssel ist ein spezifischer numerischer Wert, und der numerische Wert des Verschlüsselungsschlüssels wird basierend auf den spezifizierten Positionen und der spezifizierten Sequenz berechnet, die beim obigen Schritt S24 erhalten wurden.

[0094] Nachdem der obige Schritt S25 durchgeführt ist, veranlaßt die Geheimschlüssel festlegende Einheit **116** bei Schritt 526 den Prozessor, Klardaten (einen numerischen Wert) eines vom Benutzer eingegebenen geheimen Schlüssels zu empfangen. In der vorliegenden Ausführungsform kann eine IC-Karte, in der die Klardaten des eingegebenen geheimen Schlüssels gespeichert sind, im System **100** eingesetzt werden, um die Klardaten des geheimen Schlüssels in das System **100** einzugeben. Falls die Eingabe der Geheimschlüsseldaten einmal mit der IC-Karte durchgeführt wird, kann ein Einsetzen der IC-Karte in dem System **100** zu nachfolgenden Zeiten weggelassen werden.

[0095] Nachdem der obige Schritt S26 durchgeführt ist, veranlaßt die Verschlüsselungseinheit **117** bei Schritt S27 den Prozessor, verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen, der beim obigen Schritt S25 erhalten wurde. In der vorliegenden Ausführungsform wird beim obigen Schritt S27 ein DES-Algorithmus (engl. data encryption standard) (Datenverschlüsselungsstandard) verwendet, um verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen.

[0096] Nachdem der obige Schritt S27 durchgeführt ist, veranlaßt die Geheimschlüssel speichernde Einheit **118** bei Schritt S28 den Prozessor, die verschlüsselten Daten des geheimen Schlüssels, die beim obigen Schritt S27 erhalten wurden, in der Geheimschlüsseldatenbank **131** des Systems **100** zu speichern. In der Geheimschlüsseldatenbank **131** werden das registrierte Bildpaßwort (oder die Positionen der eingegebenen Bildpunkte und die Sequenz der Positionen, die vom Benutzer bezüglich des entsprechenden Verschlüsselungsschlüssel für den geheimen Schlüssel spezifiziert wurden) in Verbindung mit den verschlüsselten Daten des geheimen Schlüssels gespeichert.

[0097] Nachdem der obige Schritt S28 durchgeführt ist, veranlaßt die Festlegungen von Benutzerumgebungen speichernde Einheit **119** bei Schritt S29 den Prozessor, die Festlegung einer Benutzerumgebung, die bei

den obigen Schritten S21–S28 empfangen wurde, in der Datenbank **132** für Festlegungen von Benutzerumgebungen des Systems **100** zu speichern.

[0098] **Fig.** 7A und 7B zeigen die Inhalte der Geheimschlüsseldatenbank **131** und der Datenbank **132** für Festlegungen von Benutzerumgebungen, nachdem die Neueintrag-Verarbeitung von **Fig.** 6 ausgeführt ist.

[0099] Ein Benutzercode, wie in **Fig.** 7A und 7B angegeben, ist ein Code, um den Benutzer zu identifizieren, der die Neueintrag-Verarbeitung von **Fig.** 6 ausgeführt hat. Für einen spezifizierten Benutzer ist gewöhnlich ein spezifizierter Benutzercode für die Geheimschlüsseldatenbank **131** und die Datenbank **132** für Festlegungen von Benutzerumgebungen zugeordnet.

[0100] Ein Benutzername, wie in **Fig.** 7B angegeben, ist der gleiche wie der eingegebene Benutzername, der beim obigen Schritt S21 erhalten wurde. Ein Hintergrundbildcode, wie in **Fig.** 7B angegeben, ist ein Code, um das eingegebene Hintergrundbild zu spezifizieren, das beim obigen Schritt S22 erhalten wurde.

[0101] Ein geheimer Schlüssel A, wie in **Fig.** 7A angegeben, gibt die verschlüsselten Daten des geheimen Schlüssels an, der beim obigen Schritt S28 gespeichert wurde. Wie oben beschrieben wurde, werden die verschlüsselten Daten des geheimen Schlüssels, die beim obigen Schritt S27 erzeugt wurden, in der Geheimschlüsseldatenbank **131** gespeichert.

[0102] Ein Chiffre-Code, wie in **Fig.** 7A angegeben, ist ein Datenelement, das verwendet wird, um die verschlüsselten Daten in die Klardaten des geheimen Schlüssels zu entschlüsseln. Konkret wird der Chiffre-Code als eine Differenz zwischen den Klardaten (dem numerischen Wert) des geheimen Schlüssels und den verschlüsselten Daten (dem numerischen Wert) des geheimen Schlüssels berechnet.

[0103] Ein Benutzerumgebungscode, wie in **Fig.** 7B angegeben, ist ein Code, um die Festlegung einer Benutzerumgebung anzugeben, wie z. B. den verwendeten Browser, der beim obigen Schritt S21 erhalten wurde. Der Benutzerumgebungscode wird aus der Datenbank **132** für Festlegungen von Benutzerumgebungen während einer von der Bildpaßworte verarbeitenden Einheit **104** durchgeführten Verarbeitung gelesen.

[0104] Eine frühere Zugriffsadresse, wie in **Fig.** 7A angegeben, ist eine Adresse eines Zielkommunikationsdienstes, zu welchem der geheime Schlüssel von der Geheimschlüsseldatenbank **131** vorher durch die Geheimschlüssel verarbeitende Einheit **104** oder den verwendeten Browser übertragen wurde.

[0105] In der Bildpaßworte verarbeitenden Einheit **104** des Systems **100** von **Fig.** 5 sind vorgesehen eine Benutzernamen-Auswahleinheit **121**, eine Hintergrund/Musteranzeigeeinheit **122**, eine Bildpaßwort-Empfangseinheit **123**, eine Bildpaßwort-Beurteilungseinheit **124** und eine Entschlüsselungseinheit **125**.

[0106] **Fig.** 8 zeigt eine Bildpaßwortverarbeitung, die durch die Bildpaßworte verarbeitende Einheit **104** im Geheimdatenverwaltungssystem **100** durchgeführt wird.

[0107] In der vorliegenden Ausführungsform ist ein Bildpaßworte verarbeitendes Programm, das auf das Flußdiagramm von **Fig.** 8 bezogen ist (was später beschrieben wird), Programmcodeanweisungen, die im Speicher des Geheimdatenverwaltungssystems **100** gespeichert sind. Der Speicher entspricht einem computerlesbaren Medium in den Ansprüchen. Das computerlesbare Medium beinhaltet irgendeine Anweisungsspeichervorrichtung wie z. B. Magnetplatten einschließlich Disketten, optische Platten einschließlich CD-ROMs, magnetooptische Platten einschließlich MOs, Halbleiterspeicherkarten wie z. B. IC-Karten und Miniaturkarten und andere Arten von in Computer nutzbaren Vorrichtungen und Medien.

[0108] In der vorliegenden Erfindung kann der Speicher des Geheimdatenverwaltungssystems **100** codierte oder nicht codierte Anweisungen speichern. Die Anweisungen können zuerst von einer Diskette (oder einer CD-ROM) auf das Festplattenlaufwerk des Geheimdatenverwaltungssystems **100** installiert, zum RAM des Systems **100** übertragen und dann vom Prozessor des Systems **100** gelesen werden. Der Speicher des Geheimdatenverwaltungssystems **100** kann entweder alle oder einen Teil der Anweisungen speichern, die auf das Flußdiagramm von **Fig.** 8 bezogen sind.

[0109] Während einer Bildpaßwortverarbeitung von **Fig.** 8 wird vom Benutzer auf dem Anzeigemonitor durch Verwenden allein der Maus eine Authentifizierung des Benutzers für das Bildpaßwort ausgeführt.

[0110] Am Beginn der Bildpaßwortverarbeitung von **Fig.** 8 veranlaßt die Benutzernamen-Auswahleinheit **121** bei Schritt S31 den Prozessor, eine Liste registrierter Benutzernamen, die in der Datenbank **132** für Festlegungen von Benutzerumgebungen durch die Neueintrag-Verarbeitungseinheit **103** gespeichert sind, auf dem Anzeigemonitor anzuzeigen, und veranlaßt den Benutzer, einen gewünschten Benutzernamen mit der Maus einzugeben.

[0111] Nachdem der obige Schritt S31 durchgeführt ist, veranlaßt die Hintergrund/Musteranzeigeeinheit 122 bei Schritt S32 den Prozessor, das Hintergrundbild mit dem überlagerten Maschenmuster, das in der Datenbank **132** für Festlegungen von Benutzerumgebungen durch die Neueintrag-Verarbeitungseinheit **103** gespeichert ist, auf dem Anzeigemonitor anzuzeigen. Das Hintergrundbild mit dem Maschenmuster, das beim obigen Schritt S32 angezeigt wird, ist auf den eingegebenen Benutzernamen innerhalb der Datenbank **132** für Festlegungen von Benutzerumgebungen bezogen, wie in **Fig.** 7B gezeigt ist.

[0112] Nachdem der obige Schritt S32 durchgeführt ist, veranlaßt die Bildpaßwort-Empfangseinheit **123** bei Schritt S33 den Prozessor, den Benutzer zu veranlassen, ein Bildpaßwort auf dem Anzeigemonitor mit der Maus einzugeben, und Positionen von Eingabebildpunkten und eine Sequenz der Positionen zu empfangen,

die vom Benutzer gegenwärtig spezifiziert werden. Wenn der Benutzer einen spezifischen Punkt auf dem Hintergrundbild mit dem Maschenmuster anklickt, ändert sich eine Farbe oder ein Punktmuster des Anzeigemonitors an dem Punkt. Die Positionen der Eingabebildpunkte auf dem Hintergrundbild werden dem Benutzer in optischer Form geliefert, und der Benutzer kann das eingegebene Bildpaßwort auf dem Anzeigemonitor bestätigen.

[0113] Nachdem der obige Schritt S33 durchgeführt ist, veranlaßt die Bildpaßwort-Beurteilungseinheit **124** bei Schritt S34 den Prozessor, zu bestimmen, ob das Eingabebildpaßwort, das beim obigen Schritt S33 erhalten wurde, mit dem registrierten Bildpaßwort übereinstimmt, das durch die Neueintrag-Verarbeitungseinheit **103** in der Geheimschlüsseldatenbank **131** gespeichert ist.

[0114] Wenn das Ergebnis des obigen Schrittes S34 bestätigend ist, veranlaßt die Entschlüsselungseinheit **125** bei Schritt S35 den Prozessor, die aus der Geheimschlüsseldatenbank **131** ausgelesenen verschlüsselten Daten des geheimen Schlüssels in die Klardaten zu entschlüsseln. Ferner veranlaßt die Entschlüsselungseinheit **125** bei Schritt S35 den Prozessor, den Benutzerumgebungscode aus der Datenbank **132** für Festlegungen von Benutzerumgebungen zu lesen und entweder eine Verarbeitung zur Anzeige eines geheimen Schlüssels oder eine Verarbeitung für ein Browser-Link gemäß dem Inhalt des Benutzerumgebungscodes auszuführen. Wenn die Verarbeitung eines Browser-Links ausgeführt wird, veranlaßt die Entschlüsselungseinheit **125** bei Schritt S35 den Prozessor, die frühere Zugriffsadresse aus der Geheimschlüsseldatenbank **131** zu lesen und eine Adresse eines Zielkommunikationsdienstes, an den der Browser gegenwärtig die Klardaten des geheimen Schlüssels sendet, durch die frühere Zugriffsadresse festzulegen.

[0115] Wenn das Ergebnis des obigen Schritts S34 negativ ist, veranlaßt die Bildpaßworte verarbeitende Einheit **104** den Prozessor, eine Fehlermeldung auszugeben, die angibt, daß das Eingabebildpaßwort ungültig ist.

[0116] **Fig.** 9 zeigt eine Zusatzeintrag-Verarbeitung, die durch die Zusatzeintrag-Verarbeitungseinheit **105** im Geheimdatenverwaltungssystem **100** durchgeführt wird.

[0117] In der vorliegenden Ausführungsform ist ein auf das Flußdiagramm von **Fig.** 9 bezogenes Zusatzeintrag-Verarbeitungsprogramm (welches später beschrieben wird) Programmcodeanweisungen, die im Speicher des Geheimdatenverwaltungssystems **100** gespeichert sind. Der Speicher entspricht in den Ansprüchen einem computerlesbaren Medium. Das computerlesbare Medium enthält irgendeine Anweisungsspeichervorrichtung wie z. B. Magnetplatten einschließlich Disketten, optische Platten einschließlich CD-ROMs, magnetooptische Platten einschließlich MOs, Halbleiterspeicherkarten wie z. B. IC-Karten und Miniaturkarten und andere Arten von computernutzbaren Vorrichtungen und Medien.

[0118] In der vorliegenden Ausführungsform kann der Speicher des Geheimdatenverwaltungssystems **100** codierte oder nicht codierte Anweisungen speichern. Die Anweisungen können zuerst von einer Diskette (oder einem CD-ROM) auf das Festplattenlaufwerk des Geheimdatenverwaltungssystems **100** installiert, zum RAM des Systems **100** übertragen und dann vom Prozessor des Systems **100** gelesen werden. Der Speicher des Geheimdatenverwaltungssystems **100** kann entweder alle oder einen Teil der auf das Flußdiagramm von **Fig.** 9 bezogenen Anweisungen speichern.

[0119] Während der Zusatzeintrag-Verarbeitung von **Fig.** 9 werden durch den Bildpaßwort-Benutzer ein Eintrag eines zusätzlichen geheimen Schlüssels in die Geheimschlüsseldatenbank **131** und ein Eintrag einer zusätzlichen Festlegung von Benutzerumgebungen bezogen auf den Geheimschlüssel-Eintrag in die Datenbank **132** für Festlegungen von Benutzerumgebungen ausgeführt.

[0120] Am Beginn der Zusatzeintrag-Verarbeitung von **Fig.** 9 veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S41 den Prozessor, die Liste registrierter Benutzernamen, die in der Datenbank **132** für Festlegungen von Benutzerumgebungen durch die Neueintrag-Verarbeitungseinheit **103** gespeichert sind, auf dem Anzeigemonitor anzuzeigen, und veranlaßt den Benutzer, einen gewünschten Benutzernamen mit der Maus einzugeben.

[0121] Nachdem der obige Schritt S41 ausgeführt ist, veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S42 den Prozessor, das Hintergrundbild mit dem überlagerten Maschenmuster, das in der Datenbank **132** für Festlegungen von Benutzerumgebungen durch die Neueintrag-Verarbeitungseinheit **103** gespeichert ist, auf dem Anzeigemonitor anzuzeigen. Der Hintergrundbildcode, der das Hintergrundbild mit dem angezeigten Maschenmuster beim obigen Schritt S42 angibt, bezieht sich auf den eingegebenen Benutzernamen innerhalb der Datenbank **132** für Festlegungen von Benutzerumgebungen, wie in **Fig.** 7B gezeigt ist.

[0122] Nachdem der obige Schritt S42 ausgeführt ist, veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S43 den Prozessor, den Benutzer zu veranlassen, ein Bildpaßwort auf dem Anzeigemonitor mit der Maus einzugeben, und Positionen von Eingabebildpunkten und eine Sequenz der Positionen, die vom Benutzer gegenwärtig spezifiziert werden, zu empfangen. Wenn der Benutzer einen spezifischen Punkt auf dem Hintergrundbild mit dem Maschenmuster anklickt, ändert sich eine Farbe oder ein Punktmuster des Anzeigemonitors am Punkt. Die Positionen der Eingabebildpunkte auf dem Hintergrundbild werden dem Benutzer in optischer Form geliefert, und der Benutzer kann das Eingabebildpaßwort auf dem Anzeigemonitor bestätigen.

[0123] Nachdem der obige Schritt S43 durchgeführt ist, veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S44 den Prozessor zu bestimmen, ob das Eingabebildpaßwort, das beim obigen Schritt S43 erhalten wurde, mit dem registrierten Bildpaßwort übereinstimmt, das in der Geheimschlüsseldatenbank **131** durch die Neueintrag-Verarbeitungseinheit **103** gespeichert ist. Es ist möglich, daß die Bestimmung diesbezüglich, ob das Eingabebildpaßwort mit dem registrierten Bildpaßwort übereinstimmt, vorgenommen wird durch Vergleichen eines aus den spezifizierten Positionen der Eingabebildpunkte und der spezifizierten Sequenz der Positionen abgeleiteten Verschlüsselungsschlüssels mit dem aus der Geheimschlüsseldatenbank **131** gelesenen Verschlüsselungsschlüssel.

[0124] Wenn das Ergebnis des obigen Schritts S44 bestätigend ist, veranlaßt die Einheit **105** für eine Zusatreintrag-Verarbeitung bei Schritt S45 den Prozessor, die verschlüsselten Daten des geheimen Schlüssels, die aus der Geheimschlüsseldatenbank **131** gelesen wurden, in die Klardaten zu entschlüsseln.

[0125] Wenn das Ergebnis des obigen Schritts S44 negativ ist, veranlaßt die Einheit **105** für eine Zusatreintrag-Verarbeitung den Prozessor, eine Fehlermeldung auszugeben, die angibt, daß das Eingabebildpaßwort ungültig ist.

[0126] Nachdem der obige Schritt S45 ausgeführt ist, veranlaßt die Einheit **105** für eine Zusatreintrag-Verarbeitung bei Schritt S46 den Prozessor, Klardaten eines zusätzlichen, vom Benutzer eingegebenen geheimen Schlüssels zu empfangen.

[0127] Nachdem der obige Schritt S46 durchgeführt ist, veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S47 den Prozessor, verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen, der für den bestehenden geheimen Schlüssel durch die Einheit **103** für eine Neueintrag-Verarbeitung erhalten wurde. In der vorliegenden Ausführungsform wird beim obigen Schritt S47 der DES-Algorithmus verwendet, um verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen.

[0128] Nachdem der obige Schritt S47 ausgeführt ist, veranlaßt die Einheit **105** für eine Zusatreintrag-Verarbeitung bei Schritt S48 den Prozessor, die verschlüsselten Daten des geheimen Schlüssels, die beim obigen Schritt S47 erhalten wurden, in der Geheimschlüsseldatenbank **131** des Systems **100** zu speichern.

[0129] Nachdem der obige Schritt S48 durchgeführt ist, veranlaßt die Einheit **105** für eine Zusatzeintrag-Verarbeitung bei Schritt S49 den Prozessor, die Festlegung der Benutzerumgebung, die bei den obigen Schritten S41–S48 empfangen wurde, in der Datenbank **132** für Festlegungen von Benutzerumgebungen des Systems **100** zu speichern.

[0130] **Fig.** 10 zeigt die Inhalte der Geheimschlüsseldatenbank **311** in dem Geheimdatenverwaltungssystem **100**, nachdem die Zusatzeintrag-Verarbeitung von **Fig.** 9 ausgeführt ist.

[0131] Wie in **Fig.** 10 gezeigt ist, wird, nachdem die Zusatzeintrag-Verarbeitung von **Fig.** 9 durchgeführt ist, ein zusätzlicher geheimer Schlüssel B für die Benutzernamen und den Chiffre-Code, welche die gleichen wie der Benutzername und der Chiffre-Code sind, die auf den bestehenden geheimen Schlüssel A bezogen sind, in der Geheimschlüsseldatenbank **311** gespeichert. Gemäß der Funktionalität der Zusatzeintrag-Verarbeitung von **Fig.** 9 ist es möglich, daß mehrere geheime Schlüssel für ein einziges Bildpaßwort in der Geheimschlüsseldatenbank **311** registriert werden.

[0132] Wie in **Fig.** 10 gezeigt ist, wird in der Geheimschlüsseldatenbank **311** eine zusätzliche frühere Zugriffsadresse für den geheimen Schlüssel B gespeichert, die von der früheren Zugriffsadresse für den geheimen Schlüssel A verschieden ist. Das Geheimdatenverwaltungsgerät der vorliegenden Erfindung kann den geheimen Schlüssel an einen verschiedenen Zielkommunikationsdienst für einen der geheimen Schlüssel A und B senden. Falls ein zusätzliches Datenelement in der Geheimschlüsseldatenbank **131** und der Datenbank **132** für Festlegungen von Benutzerumgebungen gespeichert ist, ist es möglich, daß das Geheimdatenverwaltungsgerät und -verfahren der vorliegenden Erfindung einen zusätzlichen Kommunikationsdienst für den Benutzer liefern.

[0133] **Fig.** 11 zeigt eine Eintrag-Aktualisierungsverarbeitung, die von dem Geheimdatenverwaltungsgerät von **Fig.** 5 durchgeführt wird.

[0134] In der vorliegenden Ausführungsform ist ein auf das Flußdiagramm von **Fig.** 11 bezogenes Programm für eine Eintrag-Aktualisierungsverarbeitung (das später beschrieben wird) Programmcodeanweisungen, die im Speicher des Geheimdatenverwaltungssystems **100** gespeichert sind. Der Speicher entspricht einem computerlesbaren Medium in den Ansprüchen. Das computerlesbare Medium umfasst irgendeine Anweisungsspeichervorrichtung wie z. B. Magnetplatten einschließlich Disketten, optische Platten einschließlich CD-ROMs, magnetooptische Platten einschließlich MOs, Halbleiterspeicherkarten wie z. B. IC-Karten und Miniaturkarten und andere Arten von computernutzbaren Vorrichtungen und Medien.

[0135] In der vorliegenden Ausführungsform kann der Speicher des Geheimdatenverwaltungssystems **100** codierte oder nicht codierte Anweisungen speichern. Die Anweisungen können zuerst von einer Diskette (oder einem CD-ROM) auf das Festplattenlaufwerk des Geheimdatenverwaltungssystems **100** installiert, zum RAM des Systems **100** übertragen und dann vom Prozessor des Systems **100** gelesen werden. Der Speicher des Geheimdatenverwaltungssystems kann entweder alle oder einen Teil der auf das Flußdiagramm von **Fig.** 11

bezogenen Anweisungen speichern.

[0136] Während der Eintrag-Aktualisierungsverarbeitung von **Fig.** 11 wird ein Aktualisieren eines bestehenden Geheimschlüsseleintrags in der Geheimschlüsseldatenbank **131** vom Bildpaßwort-Benutzer ausgeführt.

[0137] Am Beginn der Eintrag-Aktualisierungsverarbeitung von **Fig.** 11 veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S51 den Prozessor, die Liste registrierter Benutzernamen, die durch die Einheit **103** zur Neueintrag-Verarbeitung in der Datenbank **132** für Festlegungen von Benutzerumgebungen gespeichert sind, auf dem Anzeigemonitor anzuzeigen, und veranlaßt den Benutzer, mit der Maus einen gewünschten Benutzernamen einzugeben.

[0138] Nachdem der obige Schritt S51 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S52 den Prozessor, das Hintergrundbild mit dem überlagerten Maschenmuster, das von der Einheit **103** für eine Neueintrag-Verarbeitung in der Datenbank **132** für Festlegungen von Benutzerumgebungen gespeichert ist, auf dem Anzeigemonitor anzuzeigen. Der Hintergrundbildcode, der das Hintergrundbild mit dem Maschenmuster angibt, angezeigt beim obigen Schritt S52, bezieht sich auf den eingegebenen Benutzernamen innerhalb der Datenbank **132** für Festlegungen von Benutzerumgebungen.

[0139] Nachdem der obige Schritt S52 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S53 den Prozessor, den Benutzer zu veranlassen, ein Bildpaßwort auf dem Anzeigemonitor mit der Maus einzugeben, und Positionen von Eingabebildpunkten und eine Sequenz der Positionen zu empfangen, die aktuell vom Benutzer spezifiziert werden. Wenn der Benutzer einen spezifischen Punkt auf dem Hintergrundbild mit dem Maschenmuster anklickt, ändert sich eine Farbe oder ein Punktmuster des Anzeigemonitors an dem Punkt. Die Positionen der Eingabebildpunkte auf dem Hintergrundbild werden in optischer Form an den Benutzer geliefert, und der Benutzer kann das Eingabebildpaßwort auf dem Anzeigemonitor bestätigen.

[0140] Nachdem der obige Schritt S53 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S54 den Prozessor zu bestimmen, ob das Eingabebildpaßwort, das beim obigen Schritt S53 erhalten wurde, mit dem registrierten Bildpaßwort übereinstimmt, das durch die Einheit **103** zur Neueintrag-Verarbeitung in der Geheimschlüsseldatenbank **131** gespeichert ist.

[0141] Wenn das Ergebnis des obigen Schritts S54 bestätigend ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S55 den Prozessor, die verschlüsselten Daten des geheimen Schlüssels, die aus der Geheimschlüsseldatenbank **131** ausgelesen wurden, in die Klardaten zu entschlüsseln.

[0142] Wenn das Ergebnis des obigen Schritts S54 negativ ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung den Prozessor, eine Fehlermeldung auszugeben, die angibt, daß das Eingabebildpaßwort ungültig ist.

[0143] Während der Eintrag-Aktualisierungsverarbeitung von **Fig.** 11 werden die folgenden Schritte S56–S64 von der Einheit **106** zur Eintrag-Aktualisierungsverarbeitung für nur den Bildpaßbenutzer durchgeführt, der bei den obigen Schritten S54 und S55 erfolgreich authentifiziert wurde.

[0144] Nachdem der obige Schritt S55 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S56 den Prozessor, eine Festlegung einer Benutzerumgebung für das Geheimdatenverwaltungssystem **100** zu empfangen, das vom Benutzer auf dem Anzeigemonitor unter Verwendung der Maus eingegeben wurde. Die vom Benutzer eingegebene Umgebungsfestlegung umfaßt einen Benutzernamen, einen verwendeten Browser und eine Browser-Link-Option.

[0145] Nachdem der obige Schritt S56 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S57 den Prozessor, ein vom Benutzer eingegebenes Hintergrundbild zu empfangen. Das eingegebene Hintergrundbild wird auf dem Anzeigemonitor angezeigt, nachdem der obige Schritt S57 während der Eintrag-Aktualisierungsverarbeitung durchgeführt ist.

[0146] Nachdem der obige Schritt S57 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S58 den Prozessor, ein vom Benutzer eingegebenes Maschenmuster zu empfangen. Das eingegebene Maschenmuster wird auf dem Hintergrundbild auf dem Anzeigemonitor während der nachfolgenden Verarbeitung der Einheit **106** zur Eintrag-Aktualisierungsverarbeitung überlagert.

[0147] Nachdem der obige Schritt S58 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S59 den Prozessor, Positionen von Eingabebildpunkten und eine Sequenz der Positionen zu empfangen, die vom Benutzer neu spezifiziert wurden (oder ein eingegebenes Bildpaßwort). Das Hintergrundbild, auf dem das Maschenmuster überlagert ist, wird auf dem Anzeigemonitor angezeigt, und der Benutzer spezifiziert durch Verwenden der Maus die Positionen der Eingabebildpunkte auf dem Hintergrundbild neu.

[0148] Nachdem der obige Schritt S59 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S60 den Prozessor, einen Verschlüsselungsschlüssel zu erzeugen, der auf den spezifizierten Positionen der Eingabebildpunkte und der spezifizierten Sequenz der Positionen basiert, die beim obigen Schritt S59 erhalten wurden. Der beim obigen Schritt S60 erhaltene Verschlüsselungsschlüssel ist ein spezifischer numerischer Wert, und der numerische Wert des Verschlüsselungsschlüssels wird basierend auf den spezifizierten Positionen und der spezifizierten Sequenz berechnet, die beim obigen Schritt S59 erhalten wur-

den.

[0149] Nachdem der obige Schritt S60 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S61 den Prozessor, Klardaten eines vom Benutzer eingegebenen geheimen Schlüssels zu empfangen. In der vorliegenden Ausführungsform kann im System **100** eine IC-Karte eingesetzt werden, in der die Klardaten des eingegebenen geheimen Schlüssels gespeichert sind, um die Klardaten des geheimen Schlüssels in das System **100** einzugeben.

[0150] Nachdem der obige Schritt S61 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S62 den Prozessor, verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen, der beim obigen Schritt S60 erhalten wurde. In der vorliegenden Ausführungsform wird beim obigen Schritt S62 der DES-Algorithmus verwendet, um verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel zu erzeugen.

[0151] Nachdem der obige Schritt S62 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S63 den Prozessor, die verschlüsselten Daten des geheimen Schlüssels, die beim obigen Schritt S62 erhalten wurden, in der Geheimschlüsseldatenbank **131** des Systems **100** zu speichern. In der Geheimschlüsseldatenbank **131** wird in Verbindung mit den verschlüsselten Daten des geheimen Schlüssels das registrierte aktualisierte Bildpaßwort (oder die Positionen der Eingabebildpunkte und die Sequenz der Positionen, die vom Benutzer bezüglich des entsprechenden Verschlüsselungsschlüssel für den geheimen Schlüssel spezifiziert wurden) gespeichert.

[0152] Nachdem der obige Schritt S63 durchgeführt ist, veranlaßt die Einheit **106** zur Eintrag-Aktualisierungsverarbeitung bei Schritt S64 den Prozessor, die Festlegung der Benutzerumgebung, die bei den obigen Schritten S56–S63 erhalten wurde, in der Datenbank **132** für Festlegungen von Benutzerumgebungen des Systems **100** zu speichern.

[0153] Als nächstes werden verschiedene Anzeigeschirme, die für den Benutzer vom Geheimdatenverwaltungssystem **100** der vorliegenden Erfindung geliefert werden, mit Verweis auf **Fig.** 12–22 beschrieben.

[0154] **Fig.** 12 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Schritt zum Festlegen von Benutzerumgebungen geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S21 von **Fig.** 6 oder dem Schritt S56 von **Fig.** 11.

[0155] Wie in **Fig.** 12 gezeigt ist, gibt der Benutzer die Festlegung einer Benutzerumgebung für das Geheimdatenverwaltungssystem **100** auf dem Anzeigemonitor unter Verwendung der Maus oder der Tastatur ein. Die vom Benutzer eingegebene Umgebungsfestlegung umfaßt einen Benutzernamen, einen verwendeten Browser und eine Browser-Link-Option. Wenn die Browser-Link-Option verwendet wird, wird über den Browser ein geheimer Schlüssel zu einem Zielkommunikationsdienst übertragen. Wenn eine Anzeigemonitorwahl verwendet wird, wird die gesamte Verarbeitung nur auf dem Anzeigemonitor durchgeführt.

[0156] **Fig.** 13 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem ein Hintergrundbild festlegenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S22 von **Fig.** 6 oder dem Schritt S57 von **Fig.** 11.

[0157] Wie in **Fig.** 13 gezeigt ist, wählt der Benutzer die registrierten Hintergrundbilder, das benutzerdefinierte Hintergrundbild oder ein anderes Hintergrundbild, das von einem externen Bildspeichermedium übertragen wurde, durch Verwenden der Maus aus. Nachdem eine Wahl eines gewünschten Hintergrundbildes vom Benutzer eingegeben ist, wird in einem Kasten des Anzeigeschirms wie in **Fig.** 13 gezeigt das eingegebene Hintergrundbild angezeigt.

[0158] **Fig.** 14 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Maschenmuster festlegenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht Schritt 523 von **Fig.** 6 oder dem Schritt S58 von **Fig.** 11.

[0159] Wie in **Fig.** 14 gezeigt ist, wählt der Benutzer eine von mehreren registrierten Maschengrößen und eine von registrierten Maschenmusterfarben aus. Wenn vom Benutzer gewünschte Maschenmusterwahlen eingegeben sind, wird das eingegebene Maschenmuster auf dem eingegebenen Hintergrundbild im Kasten des Anzeigeschirms wie in **Fig.** 14 gezeigt überlagert. Der Benutzer kann bestätigen, daß das gewünschte Maschenmuster im Geheimdatenverwaltungssystem **100** ausgewählt ist.

[0160] Für **Fig.** 15 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Positions/Sequenzdaten festlegenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S23 von **Fig.** 6 oder dem Schritt S58 von **Fig.** 11.

[0161] Wie in **Fig.** 15 gezeigt ist, wählt durch Verwenden der Maus der Benutzer eine von mehreren registrierten Anzahlen Ziffern des Eingabebildpaßwortes aus und spezifiziert Positionen von Eingabebildpunkten und eine Sequenz der Positionen auf dem Hintergrundbild mit dem auf dem Anzeigemonitor angezeigten Maschenmuster. Die Zahl der Positionen, die der Benutzer spezifizieren kann, hängt von der ausgewählten Anzahl Ziffern des Eingabebildpaßwortes ab. Falls die Anzahl der vom Benutzer spezifizierten Positionen die ausgewählte Anzahl Ziffern überschreitet, wird eine Fehlermeldung ausgegeben. Falls die Anzahl der vom Benutzer spezifizierten Positionen geringer als die ausgewählte Zahl von Ziffern ist und ein OK-Knopf angeklickt

wird, wird eine Fehlermeldung ausgegeben, die den Benutzer veranlaßt, alle Eingabebildpunkte auf dem Hintergrundbild zu spezifizieren.

[0162] Wenn ein spezifischer Punkt auf dem Hintergrundbild im Kasten des Anzeigeschirms vom Benutzer angeklickt wird, ändert sich eine Farbe oder ein Punktmuster des Anzeigemonitors an dem Punkt innerhalb des Hintergrundbildes. Die Positionen der Eingabebildpunkte, die vom Benutzer auf dem Hintergrundbild spezifiziert wurden, werden in optischer Form an den Benutzer geliefert. Im Anzeigeschirm von **Fig.** 15 wird ferner die Sequenz der vom Benutzer spezifizierten Positionen durch eine Reihe kleiner Kästen mit verschiedenen Punktmustern angegeben, die den Punktmustern des Anzeigemonitors an den Eingabebildpunkten auf dem Hintergrundbild entsprechen. Daher kann der Benutzer die spezifizierten Positionen der Eingabebildpunkte und die spezifizierte Sequenz der Positionen (oder das Eingabebildpaßwort) auf dem Anzeigemonitor bestätigen.

[0163] **Fig.** 16 ist ein Diagramm zum Erläutern einer Konfiguration der Verschlüsselungsschlüssel erzeugenden Einheit **115** des Geheimdatenverwaltungsgeräts von **Fig.** 5. Die Konfiguration der Verschlüsselungsschlüssel erzeugenden Einheit **115** wird nun mit Verweis auf **Fig.** 16 beschrieben.

[0164] Im Beispiel von **Fig.** 16 ist die Anzahl von Ziffern des Bildpaßwortes auf 4 festgelegt, und das Maschenmuster wird in einer 8 × 10-Matrixformation geliefert. Das heißt, das Hintergrundbild besteht aus einer Matrix von Bildpunkten mit 8 Reihen und 10 Spalten, und die Positionen der vier Eingabebildpunkte und die Sequenz der Positionen sind wie in **Fig.** 16 gezeigt spezifiziert.

[0165] Wie in **Fig.** 16 gezeigt ist, wird für das Hintergrundbild des vorliegenden Beispiels ein (x,y)-Koordinatensystem definiert. Die Position des Bildpunktes an der linken obersten Ecke des Hintergrundbildes ist definiert durch (1,1), und die Position des Bildpunktes an der rechten oberen Ecke des Hintergrundbildes ist definiert durch (10,1). Man nehme an, daß die vier Eingabebildpunkte auf dem Hintergrundbild vom Benutzer in der spezifizierten Sequenz angeklickt werden. Der durch die Verschlüsselungsschlüssel erzeugende Einheit **115** der vorliegenden Ausführungsform in diesem Beispiel erzeugte Verschlüsselungsschlüssel ist angegeben durch die spezifizierte Sequenz der vier (x,y)-Koordinaten: (1,2), (3,8), (7,8) und (10,2).

[0166] In der vorliegenden Ausführungsform erzeugt die Verschlüsselungseinheit **117** verschlüsselte Daten des eingegebenen geheimen Schlüssels basierend auf der spezifizierten Sequenz der (x,y)-Koordinaten gemäß dem DES-Algorithmus. Der DES-Algorithmus führt eine numerische Eins-zu-Eins-Buchstabensubstitution des eingegebenen geheimen Schlüssels gemäß der spezifizierten Sequenz der (x,y)-Koordinaten durch. Zuerst wird der numerische Buchstabe der y-Koordinate für den numerischen Buchstaben der x-Koordinate substituiert.

[0167] Zweitens wird der numerische Buchstabe der x-Koordinate für den numerischen Buchstaben der y-Koordinate substituiert. Die beiden Substitutionsprozeduren werden auch gemäß der spezifizierten Sequenz abwechselnd wiederholt.

[0168] Im Beispiel von **Fig.** 16 wird die Verschlüsselung des eingegebenen geheimen Schlüssels, um verschlüsselte Daten des eingegebenen geheimen Schlüssels zu erzeugen, durch die Verschlüsselungseinheit **117** der vorliegenden Ausführungsform wie folgt ausgeführt.

[0169] Man nehme an, daß der eingegebene geheime Schlüssel **1234** ist. Die spezifizierte Sequenz der vier (x,y)-Koordinaten ist gegeben als (1,2), (3,8), (7,8) und (10,2). Da der erste Eingabepunkt durch (1,2) angegeben ist, wird der Buchstabe " 2" für den Buchstaben "1" substituiert. Da der zweite Eingabepunkt durch (3,8) angegeben ist, wird der Buchstabe "3" für den Buchstaben "8" substituiert. Der eingegebene geheime Schlüssel schließt jedoch nicht den Buchstaben "8" ein, und es wird keine Substitution durchgeführt. Da der dritte Eingabepunkt durch (7,8) angegeben ist, wird der Buchstabe "8" für den Buchstaben "7" substituiert. Der eingegebene geheime Schlüssel enthält nicht den Buchstaben "7", und es wird keine Substitution durchgeführt. Da der vierte Eingabepunkt angegeben ist durch (10,2), wird der Buchstabe "0" für den Buchstaben "2" substituiert. Folglich wird die obige Verschlüsselung wie folgt durchgeführt.

Eingegebener geheimer Schlüssel	1234
(1,2)	2234
(3,8)	2234
(7,8)	2234
(10,2)	0034

[0170] Gemäß dem oben beschriebenen Verschlüsselungsalgorithmus ist die Länge der verschlüsselten Daten die gleiche wie die Länge des eingegebenen geheimen Schlüssels, und die Längen der Geheimschlüsseldaten, bevor und nachdem die Verschlüsselung durchgeführt ist, bleiben unverändert.

[0171] In der vorliegenden Ausführungsform wird ferner die Entschlüsselung, um die Klardaten des geheimen Schlüssels aus den verschlüsselten Daten des geheimen Schlüssels zu erzeugen, von der Entschlüsselungseinheit **125** durch Addieren eines Chiffre-Codes zu den verschlüsselten Daten durchgeführt. Wie oben beschrieben wurde, wird der Chiffre-Code als die Differenz zwischen den Klardaten des geheimen Schlüssels

und den verschlüsselten Daten des geheimen Schlüssels berechnet. Im Beispiel von **Fig.** 16 wird der Chiffre-Code wie in der Formel 1200 = 1234 – 0034 berechnet. Daher wird die Entschlüsselung, um die Klardaten (1234) aus den Chiffre-Daten (0034) in diesem Beispiel zu erzeugen, von der Entschlüsselungseinheit **125** durch Addieren von 1200 zu 0034 durchgeführt.

[0172] **Fig.** 17 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Verschlüsselungsschlüssel erzeugenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S25 von **Fig.** 6 oder dem Schritt S60 von **Fig.** 11.

[0173] Wie in **Fig.** 17 gezeigt ist, wird, nachdem die obigen Schritte S21–S24 von **Fig.** 6 oder die obigen Schritte S56–S59 erfolgreich ausgeführt sind, der Benutzer auf dem Anzeigemonitor von dem Geheimdatenverwaltungssystem **100** informiert, daß ein dem Benutzer eigener Verschlüsselungsschlüssel durch die Positionen der Eingabebildpunkte und die Sequenz der vom Benutzer spezifizierten Positionen erzeugt ist.

[0174] **Fig.** 18 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem geheime Schlüssel festlegenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S26 von **Fig.** 6 oder dem Schritt S61 von **Fig.** 11.

[0175] Wie in **Fig.** 18 gezeigt ist, wird der Benutzer veranlaßt, eine von mehreren Geheimschlüssel-Eingabeverfahren auf dem Anzeigeschirm auszuwählen. Die mehreren Geheimschlüssel-Eingabeverfahren umfassen: (1) einen durch eine IC-Karte eingegebenen geheimen Schlüssel; (2) einen durch eine Dateiübertragung eingegebenen geheimen Schlüssel; und (3) einen durch eine Tastatur eingegebenen geheimen Schlüssel. Nachdem der Benutzer das Eingabeverfahren auswählt und den OK-Knopf drückt, werden vom System **100** die Klardaten des vom Benutzer eingegebenen geheimen Schlüssels empfangen.

[0176] **Fig.** 19 zeigt einen Anzeigschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem registrierte Benutzernamen festlegenden Schritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S31 von **Fig.** B.

[0177] Während der Bildpaßwortverarbeitung von **Fig.** 8 wird vom Benutzer auf dem Anzeigemonitor durch allein Verwenden der Maus eine Authentifizierung des Benutzers für das Bildpaßwort ausgeführt. Das Geheimdatenverwaltungsgerät der vorliegenden Erfindung kann eine erhöhte Bedienbarkeit für den Benutzer und angemessene Sicherheit für die geheime Information liefern.

[0178] Wie in **Fig.** 19 gezeigt ist, wird bei dem registrierte Benutzernamen festlegenden Schritt der Benutzer veranlaßt, einen der registrierten Benutzernamen in der Benutzernamenliste auf dem Anzeigemonitor auszuwählen.

[0179] **Fig.** 20 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Hintergrund/Musteranzeigeschritt geliefert wird. Dieser Anzeigeschirm entspricht den Schritten S32 und S33 von **Fig.** B.

[0180] Wie in **Fig.** 20 gezeigt ist, wird auf dem Anzeigemonitor das Hintergrundbild mit dem vom Benutzer vorher festgelegten Maschenmuster angezeigt. Im Beispiel von **Fig.** 20 kann der Benutzer eine Maschenmuster-Anzeigeoption ("AN") oder eine Maschenmuster-Nichtanzeigeoption ("AUS") auswählen. Beim Bildpaßwort-Empfangsschritt wird der Benutzer veranlaßt, die Positionen der Eingabebildpunkte auf dem Hintergrundbild und die Sequenz der Positionen durch Verwenden der Maus zu spezifizieren. Nachdem der Benutzer den OK-Knopf drückt, werden vom System **100** die Positionen der Eingabebildpunkte und die Sequenz der Position, die vom Benutzer spezifiziert wurden, empfangen.

[0181] **Fig.** 21 zeigt einen Anzeigeschirm, der vom Geheimdatenverwaltungsgerät von **Fig.** 5 bei einem Bildpaßwort-Empfangsschritt geliefert wird. Dieser Anzeigeschirm entspricht dem Schritt S34 von **Fig.** B.

[0182] Wie in **Fig.** 21 gezeigt ist, wird, wenn das Ergebnis des Schritts S34 bestätigend ist, dem Benutzer vom System **100** auf dem Anzeigemonitor mitgeteilt, daß das vom Benutzer eingegebene Bildpaßwort vom System **100** akzeptiert ist. Ferner wird der Benutzer veranlaßt, durch Verwenden der Maus eines von mehreren Geheimschlüssel-Übertragungsverfahren auf dem Anzeigemonitor auszuwählen. Die mehreren Geheimschlüssel-Übertragungsverfahren umfassen: (1) eine Übertragung der Geheimschlüsseldaten durch den Browser; (2) eine Übertragung der Geheimschlüsseldaten zum Anzeigemonitor; und (3) eine Übertragung der Geheimschlüsseldaten zu einer Datei innerhalb des Speichermediums des Systems **100**. Nachdem der Benutzer das Geheimschlüssel-Übertragungsverfahren auswählt und den OK-Knopf drückt, werden die Klardaten des geheimen Schlüssels vom System **100** gemäß dem ausgewählten Verfahren übertragen.

[0183] **Fig.** 22A und 22B zeigen Anzeigeschirme, die von einem Browser geliefert werden, wenn die Browser-Link-Option verwendet wird.

[0184] Der Anzeigeschirm von **Fig.** 22A wird vom Browser geliefert, nachdem die Authentifizierung des Benutzers für das Bildpaßwort ausgeführt ist. Es wird vorgeschlagen, daß die Browser-Link-Option verwendet wird. Wenn ein Digitalsignaturknopf im Anzeigeschirm angeklickt wird, wird der Benutzer veranlaßt, ein Ziel einzugeben, zu dem die Geheimschlüssel übertragen werden. Die vom Browser übertragenen Geheimschlüsseldaten werden in das vom Benutzer eingegebene Ziel gespeichert.

[0185] Wenn der vom Benutzer gespeicherte geheime Schlüssel vorher nicht verwendet wird, wird die Bildpaßwortverarbeitung gestartet, die in einem Icon des Anzeigeschirms plaziert ist. Der Anzeigeschirm von

Fig. 22B wird in solch einem Fall vom Browser geliefert. Im Anzeigeschirm von **Fig.** 22B wird der Benutzer veranlaßt, einen der von mehreren Zertifizierungsautoritäten ausgegebenen und dem Benutzer gehörenden geheimen Schlüssel als den geheimen Schlüssel auszuwählen, den der Benutzer gegenwärtig verwenden möchte.

[0186] Nachdem die Daten des ausgewählten geheimen Schlüssels im Anzeigeschirm von **Fig.** 22B zum Ziel übertragen sind, wird die frühere Zugriffsadresse für den in der Geheimschlüsseldatenbank **131** gespeicherten entsprechenden geheimen Schlüssel so aktualisiert, daß die Adresse des zugehörigen Zielkommunikationsdienstes zusammen mit dem geheimen Schlüssel modifiziert wird. Ferner kann ein Datenelement der zugehörigen Zertifizierungsautorität zur Geheimschlüsseldatenbank **131** addiert werden. Gemäß dieser Modifikation kann das Geheimdatenverwaltungsgerät der vorliegenden Ausführungsform eine erhöhte Bedienbarkeit für den Benutzer und angemessene Sicherheit für die Geheiminformation liefern. Es ist nicht notwendig, daß sich der Benutzer sowohl an den geheimen Schlüssel als auch die zugehörige Zertifizierungsautorität für jeden Kommunikationsdienst erinnern muß.

[0187] Die vorliegende Ausführungsform ist ferner nicht auf die oben beschriebene Ausführungsform begrenzt, und Variationen und Modifikationen können vorgenommen werden, ohne vom Umfang der vorliegenden Erfindung wie in den Ansprüchen definiert abzuweichen.

Patentansprüche

1. Geheimdatenverwaltungsgerät zum Steuern eines geheimen Schlüssels, so daß der geheime Schlüssel vertraulich gehalten wird, welches Geheimdatenverwaltungsgerät aufweist:
eine Bildanzeigeeinheit (**10**; **32**) zum Anzeigen eines Bildes auf einem Anzeigemonitor (**4**);
eine Positions/Sequenzeingabeeinheit (12; 40) zum Eingeben von Positionen von Eingabebildpunkten auf dem Bild unter Verwendung einer Eingabevorrichtung (**6**) und zum Eingeben einer Sequenz der Positionen unter Verwendung der Eingabevorrichtung;
eine Verschlüsselungseinheit (**14**; **42**) zum Erzeugen verschlüsselter Daten des geheimen Schlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit (12; 40);
eine Geheimdatenspeichereinheit (**16**; **50**) zum Speichern der verschlüsselten Daten des geheimen Schlüssels von der Verschlüsselungseinheit (**14**; **42**) in einem Speichermedium;
eine Zugriffserlaubniseinheit (**18**; **60**) zum Erlauben eines Zugriffs auf den geheimen Schlüssel, der in dem Speichermedium gespeichert ist, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die unter Verwendung der Eingabevorrichtung zu einer Zeit des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit (**12**; **40**) übereinstimmen; und
eine Entschlüsselungseinheit (**20**; **66**) zum Erzeugen von Klardaten des geheimen Schlüssels aus den im Speichermedium gespeicherten verschlüsselten Daten, wenn der Zugriff durch die Zugriffserlaubniseinheit (**18**; **60**) erlaubt wird.

2. Geheimdatenverwaltungsgerät nach Anspruch 1, dadurch gekennzeichnet, daß die Verschlüsselungseinheit (**42**) aufweist:
eine Verschlüsselungsschlüssel erzeugende Einheit (**44**) zum Erzeugen eines Verschlüsselungsschlüssels auf der Basis der Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit (**40**); und
eine Geheimschlüssel-Verschlüsselungseinheit (**46**) zum Erzeugen verschlüsselter Daten des geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel von der Verschlüsselungsschlüssel erzeugenden Einheit (**44**).

3. Geheimdatenverwaltungsgerät nach Anspruch 2, dadurch gekennzeichnet, daß die Verschlüsselschlüssel erzeugende Einheit (**44**) einen Wert des Verschlüsselungsschlüssels basierend auf den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit (**40**) berechnet und daß die Geheimschlüssel-Verschlüsselungseinheit (**46**) eine Eins-zu-Eins-Buchstabensubstitution des eingegebenen geheimen Schlüssels gemäß dem berechneten Wert von der Verschlüsselungsschlüssel erzeugenden Einheit (**44**) durchführt.

4. Geheimdatenverwaltungsgerät nach einem der vorhergehenden Ansprüche, worin der Geheimschlüssel durch eine Zertifizierungsautorität ausgegeben wird.

5. Geheimdatenverwaltungsgerät nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Bildanzeigeeinheit (**32**) ein registriertes Bild (**34**) auf dem Anzeigemonitor (**4**) anzeigt.

6. Geheimdatenverwaltungsgerät nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Bildanzeigeeinheit (**32**) ein benutzerdefiniertes Bild (**36**) auf dem Anzeigemonitor (**4**) anzeigt.

7. Geheimdatenverwaltungsgerät nach Anspruch 6, worin das Speichermedium ein erstes Speichermedium ist, dadurch gekennzeichnet, daß die Bildanzeigeeinheit (**32**) ein benutzerdefiniertes Bild, das von einem zweiten Speichermedium übertragen wurde, auf dem Anzeigemonitor (**4**) anzeigt, welches zweite Speichermedium vom ersten Speichermedium getrennt ist.

8. Geheimdatenverwaltungsgerät nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Gerät ferner eine Maschenmusteranzeigeeinheit (**38**) aufweist, um ein auf dem Bild überlagertes Maschenmuster auf dem Anzeigemonitor (**4**) anzuzeigen, welches Maschenmuster eine auswählbare Maschengröße und eine auswählbare Maschenmusterfarbe hat.

9. Geheimdatenverwaltungsgerät nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Verschlüsselungseinheit (**42**) verschlüsselte Daten mehrerer geheimer Schlüssel erzeugt, wenn identische Positionen von Eingabebildpunkten auf dem Bild und eine identische Sequenz der Positionen unter Verwendung der Eingabevorrichtung (**6**) spezifiziert und durch die Positions/Sequenzeingabeeinheit (**40**) eingegeben werden, und daß die Zugriffserlaubniseinheit (**60**) einen Zugriff auf die mehreren geheimen Schlüssel erlaubt, wenn die identischen Positionen und die identische Sequenz unter Verwendung der Eingabevorrichtung zu einem Zeitpunkt des Zugriffs nachfolgend spezifiziert werden.

10. Geheimdatenverwaltungsgerät nach einem der vorhergehenden Ansprüche, worin das Speichermedium ein erstes Speichermedium ist, dadurch gekennzeichnet, daß das Gerät ferner eine zweite Eingabeeinheit (**68**) aufweist, um Benutzerdaten (**54**) und Benutrerumgebungsdaten (**56**) einzugeben, die durch einen Benutzer spezifiziert werden, und daß die Geheimdatenspeichereinheit (**50**) die Benutzerdaten und die Benutrerumgebungsdaten im ersten Speichermedium zusätzlich zu den verschlüsselten Daten (**52**) des geheimen Schlüssels speichert.

11. Geheimdatenverwaltungsgerät nach Anspruch 10, worin das Speichermedium ein erstes Speichermedium ist, dadurch gekennzeichnet, daß die Zugriffserlaubniseinheit (**60**) aufweist:
eine Zugriffsmöglichkeit-Beurteilungseinheit (**62**), um zu bestimmen, ob Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die unter Verwendung der Eingabevorrichtung zu einem Zeitpunkt des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der Positions/Sequenzeingabeeinheit (**40**) übereinstimmen; und
eine Geheimschlüssel-Auswahleinheit (**40**) zum Lesen der Benutzerdaten und der Benutrerumgebungsdaten zusätzlich zu den verschlüsselten Daten des geheimen Schlüssels vom ersten Speichermedium, wenn der Zugriff auf den geheimen Schlüssel erlaubt ist.

12. Verfahren zum Steuern eines geheimen Schlüssels, so daß der geheime Schlüssel vertraulich gehalten wird, welches Verfahren die Schritte aufweist:
Eingeben von Benutzerdaten (**54**) und Benutrerumgebungsdaten (**56**), die durch einen Benutzer spezifiziert werden;
Festlegen eines Bildes, das auf einem Anzeigemonitor (**4**) angezeigt werden soll;
Anzeigen des Bildes auf dem Anzeigemonitor und Eingeben von Positionen von Eingabebildpunkten auf dem angezeigten Bild, die durch den Benutzer spezifiziert werden, und einer Sequenz der Positionen, die durch den Benutzer spezifiziert wird;
Erzeugen eines Verschlüsselungsschlüssels basierend auf den spezifizierten Positionen und der spezifizierten Sequenz;
Erzeugen verschlüsselter Daten des geheimen Schlüssels basierend auf dem Verschlüsselungsschlüssel; und
Speichern der verschlüsselten Daten (**52**) des geheimen Schlüssels, der Benutzerdaten (**54**) und der Benutrerumgebungsdaten (**56**) in einem Speichermedium, worin die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten miteinander zusammenhängen und die verschlüsselten Daten, die Benutzerdaten und die Benutzerumgebungsdaten im Speichermedium registriert sind.

13. Verfahren nach Anspruch 12, ferner aufweisend die Schritte:
Eingeben der Benutzerdaten, die nachfolgend durch den Benutzer spezifiziert werden;
Anzeigen des Bildes auf dem Anzeigemonitor (**4**) und Eingeben von Positionen von Eingabebildpunkten auf dem angezeigten Bild, die durch den Benutzer nachfolgend spezifiziert werden, und einer Sequenz der Positionen, die durch den Benutzer nachfolgend spezifiziert wird;
Bestimmen, ob die nachfolgend spezifizierten Positionen und die Sequenz mit den vorher spezifizierten Positionen und der Sequenz übereinstimmen; und
Erzeugen von Klardaten des geheimen Schlüssels aus den verschlüsselten Daten, die im Speichermedium gespeichert sind und mit den Benutzerdaten zusammenhängen, und Erlauben eines Zugriffs auf den geheimen

Schlüssel gemäß den Benutrerumgebungsdaten, die mit dem geheimen Schlüssel zusammenhängen, wenn der Bestimmungsschritt die Übereinstimmung ergibt; und
Sperren des Zugriffs auf den geheimen Schlüssel, wenn der Bestimmungsschritt die Übereinstimmung nicht ergibt.

14. Computerlesbares Medium, das einen Programmcode speichert, um einen Prozessor zu veranlassen, eine Geheimdatenverarbeitung auszuführen, welche einen geheimen Schlüssel steuert, so daß der geheime Schlüssel in einem Geheimdatenverwaltungsgerät vertraulich gehalten wird, aufweisend:
eine erste Programmcodevorrichtung, die den Prozessor veranlaßt, ein Bild auf einem Anzeigemonitor anzuzeigen;
eine zweite Programmcodevorrichtung, die den Prozessor veranlaßt, Positionen von Eingabebildpunkten auf dem Bild, die unter Verwendung einer Eingabevorrichtung spezifiziert werden, einzugeben und eine Sequenz der Positionen einzugeben, die unter Verwendung der Eingabevorrichtung spezifiziert wird;
eine dritte Programmcodevorrichtung, die den Prozessor veranlaßt, verschlüsselte Daten des geheimen Schlüssels basierend auf den Positionen und der Sequenz von der zweiten Programmcodevorrichtung zu erzeugen;
eine vierte Programmcodevorrichtung, die den Prozessor veranlaßt, die verschlüsselten Daten des geheimen Schlüssels von der dritten Programmcodevorrichtung in einem ersten Speichermedium zu speichern;
eine fünfte Programmcodevorrichtung, die den Prozessor veranlaßt, einen Zugriff auf den im ersten Speichermedium gespeicherten geheimen Schlüssel zu erlauben, wenn Positionen von Eingabebildpunkten auf dem Bild und eine Sequenz der Positionen, die unter Verwendung der Eingabevorrichtung zu einem Zeitpunkt des Zugriffs nachfolgend spezifiziert werden, mit den Positionen und der Sequenz von der zweiten Programmcodevorrichtung übereinstimmen; und
eine sechste Programmcodevorrichtung, die den Prozessor veranlaßt, Klardaten des geheimen Schlüssels aus den im ersten Speichermedium gespeicherten verschlüsselten Daten zu erzeugen, wenn der Zugriff erlaubt wird.

Es folgen 20 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

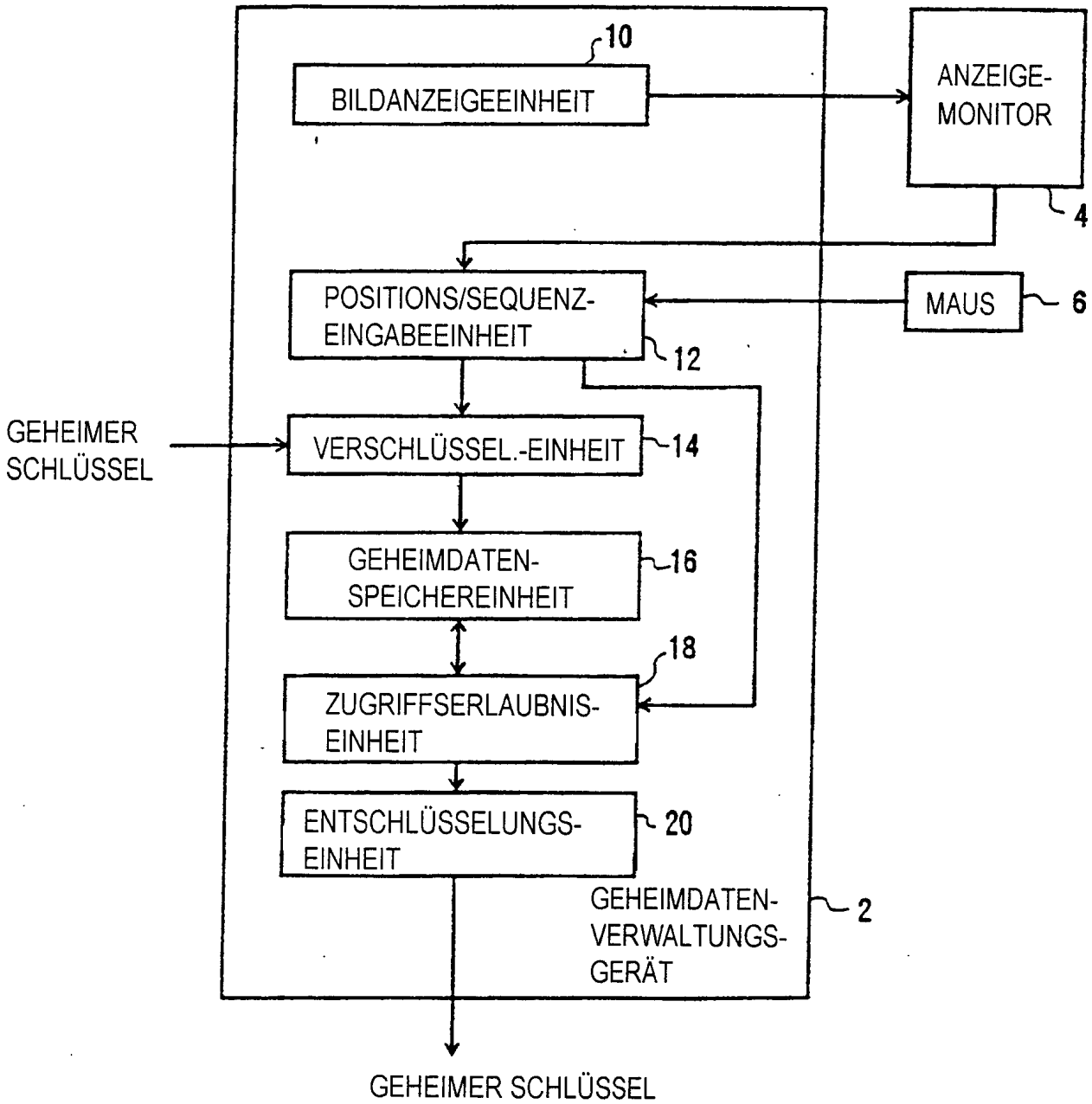


FIG. 2

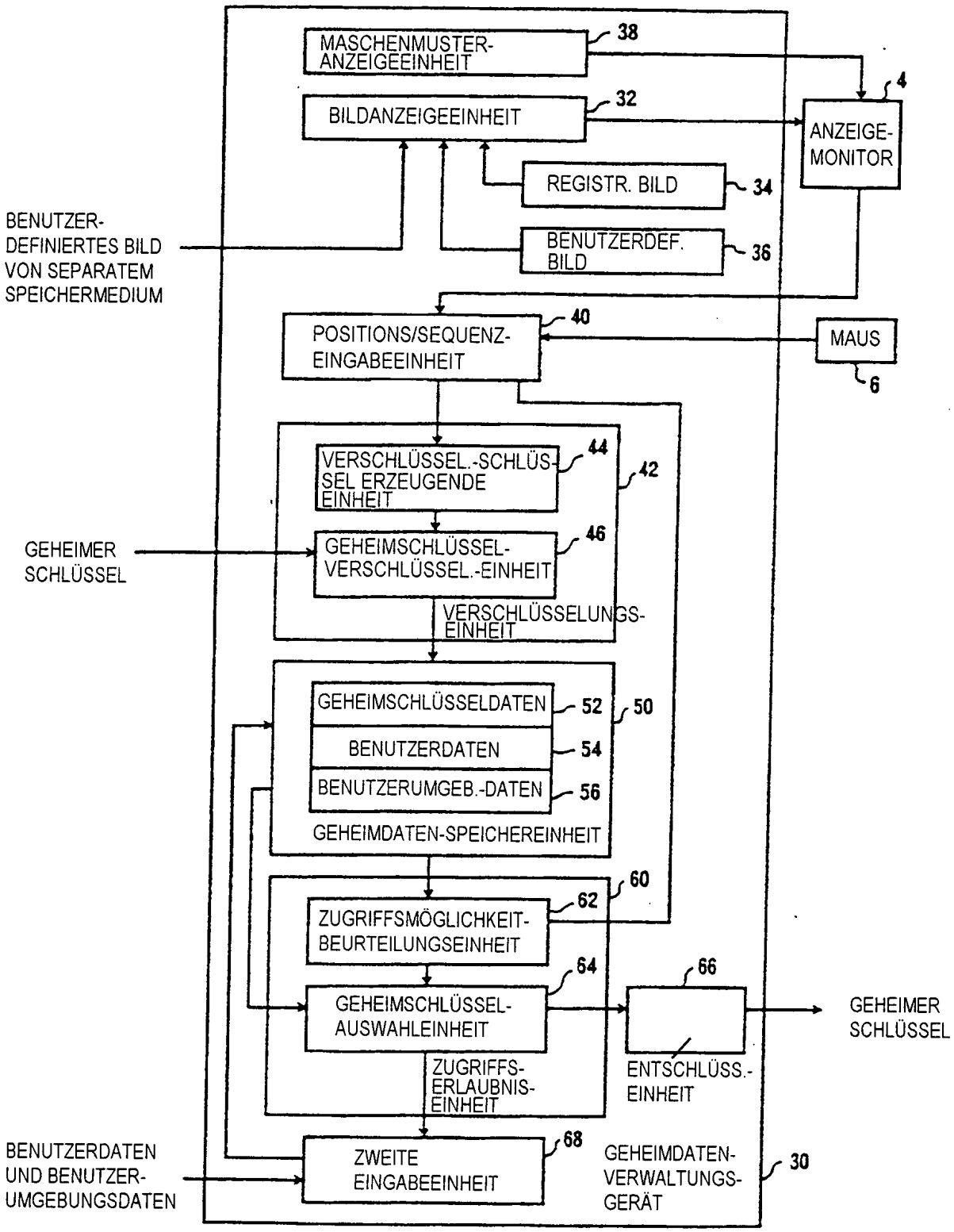

MASCHENMUSTER-ANZEIGEEINHEIT
38
BILDANZEIGEEINHEIT
32
4
ANZEIGE-MONITOR
REGISTR. BILD
34
BENUTZER-DEFINIERTES BILD VON SEPARATEM SPEICHERMEDIUM
BENUTZERDEF. BILD
36
POSITIONS/SEQUENZ-EINGABEEINHEIT
40
MAUS
6
VERSCHLÜSSEL.-SCHLÜSSEL ERZEUGENDE EINHEIT
44
42
GEHEIMER SCHLÜSSEL
GEHEIMSCHLÜSSEL-VERSCHLÜSSEL.-EINHEIT
46
VERSCHLÜSSELUNGS-EINHEIT
GEHEIMSCHLÜSSELDATEN
52
50
BENUTZERDATEN
54
BENUTZERUMGEB.-DATEN
56
GEHEIMDATEN-SPEICHEREINHEIT
60
ZUGRIFFSMÖGLICHKEIT-BEURTEILUNGSEINHEIT
62
64
66
GEHEIMSCHLÜSSEL-AUSWAHLEINHEIT
GEHEIMER SCHLÜSSEL
ZUGRIFFS-ERLAUBNIS-EINHEIT
ENTSCHLÜSS.-EINHEIT
BENUTZERDATEN UND BENUTZER-UMGEBUNGSDATEN
ZWEITE EINGABEEINHEIT
68
GEHEIMDATEN-VERWALTUNGS-GERÄT
30

FIG. 3

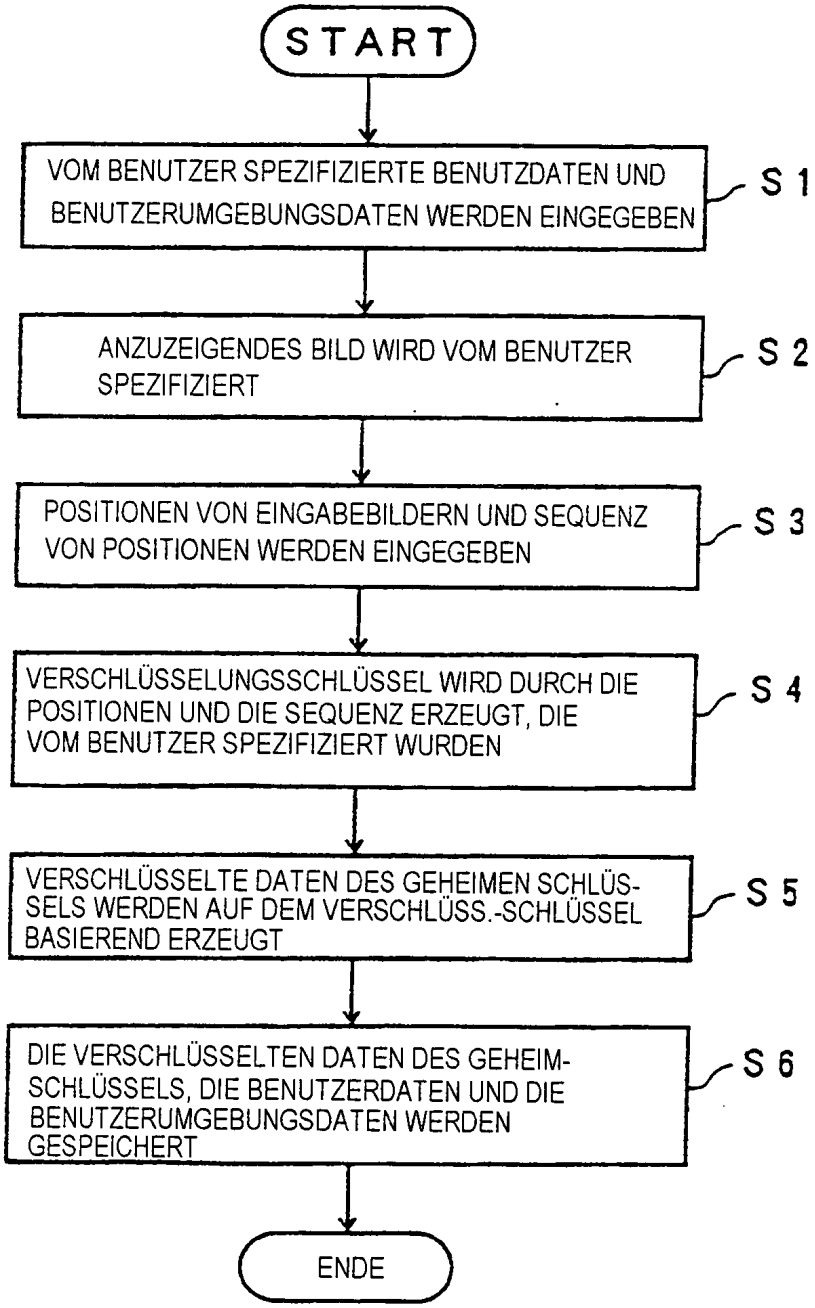

START
VOM BENUTZER SPEZIFIZIERTE BENUTZDATEN UND BENUTZERUMGEBUNGSDATEN WERDEN EINGEGEBEN
S 1
ANZUZEIGENDES BILD WIRD VOM BENUTZER SPEZIFIZIERT
S 2
POSITIONEN VON EINGABEBILDERN UND SEQUENZ VON POSITIONEN WERDEN EINGEGEBEN
S 3
VERSCHLÜSSELUNGSSCHLÜSSEL WIRD DURCH DIE POSITIONEN UND DIE SEQUENZ ERZEUGT, DIE VOM BENUTZER SPEZIFIZIERT WURDEN
S 4
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN AUF DEM VERSCHLÜSS.-SCHLÜSSEL BASIEREND ERZEUGT
S 5
DIE VERSCHLÜSSELTEN DATEN DES GEHEIMSCHLÜSSELS, DIE BENUTZERDATEN UND DIE BENUTZERUMGEBUNGSDATEN WERDEN GESPEICHERT
S 6
ENDE

FIG. 4

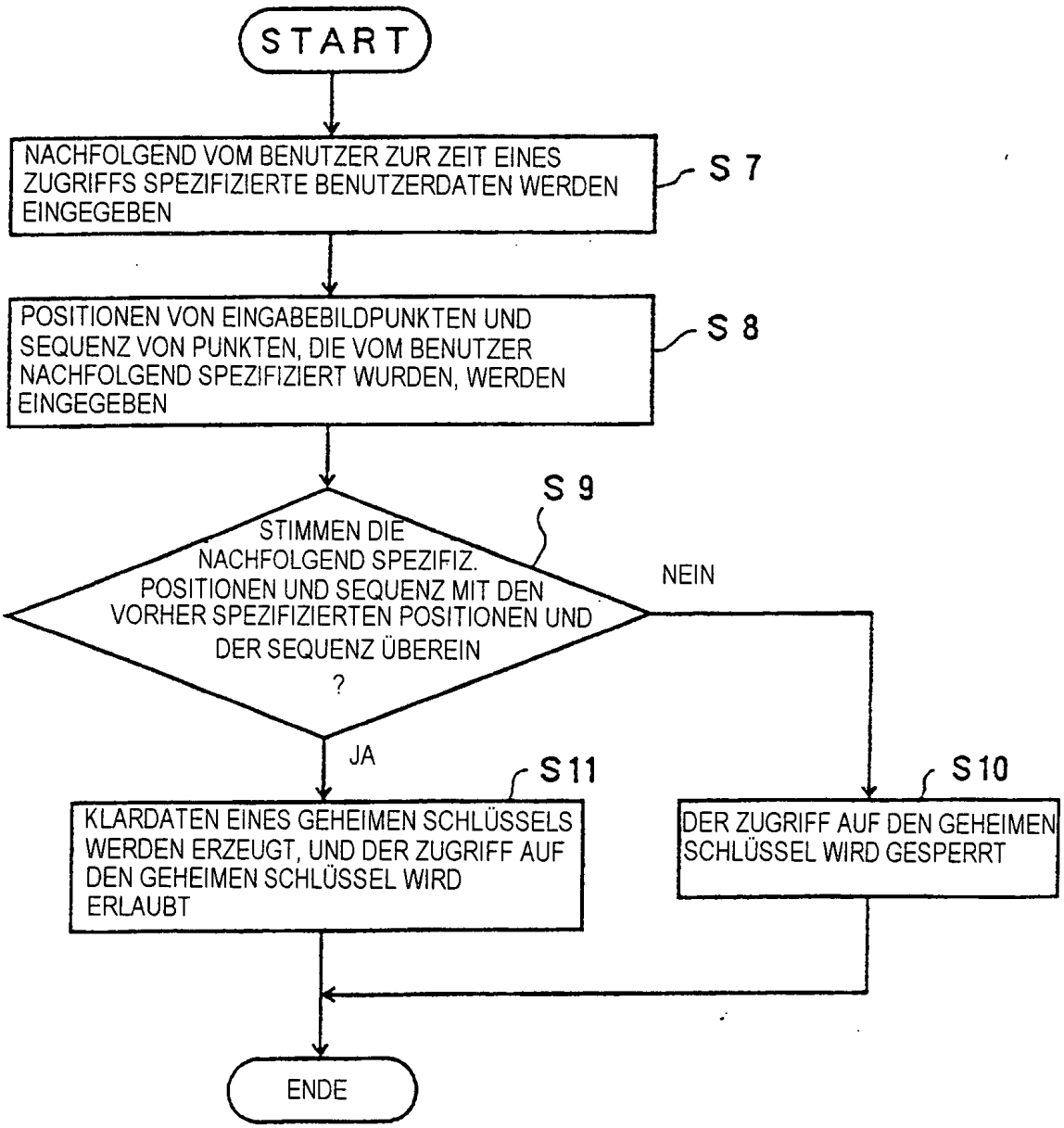

START
NACHFOLGEND VOM BENUTZER ZUR ZEIT EINES ZUGRIFFS SPEZIFIZIERTE BENUTZERDATEN WERDEN EINGEGEBEN
S 7
POSITIONEN VON EINGABEBILDPUNKTEN UND SEQUENZ VON PUNKTEN, DIE VOM BENUTZER NACHFOLGEND SPEZIFIZIERT WURDEN, WERDEN EINGEGEBEN
S 8
S 9
STIMMEN DIE NACHFOLGEND SPEZIFIZ. POSITIONEN UND SEQUENZ MIT DEN VORHER SPEZIFIZIERTEN POSITIONEN UND DER SEQUENZ ÜBEREIN ?
NEIN
JA
S 11
KLARDATEN EINES GEHEIMEN SCHLÜSSELS WERDEN ERZEUGT, UND DER ZUGRIFF AUF DEN GEHEIMEN SCHLÜSSEL WIRD ERLAUBT
S 10
DER ZUGRIFF AUF DEN GEHEIMEN SCHLÜSSEL WIRD GESPERRT
ENDE

FIG. 5

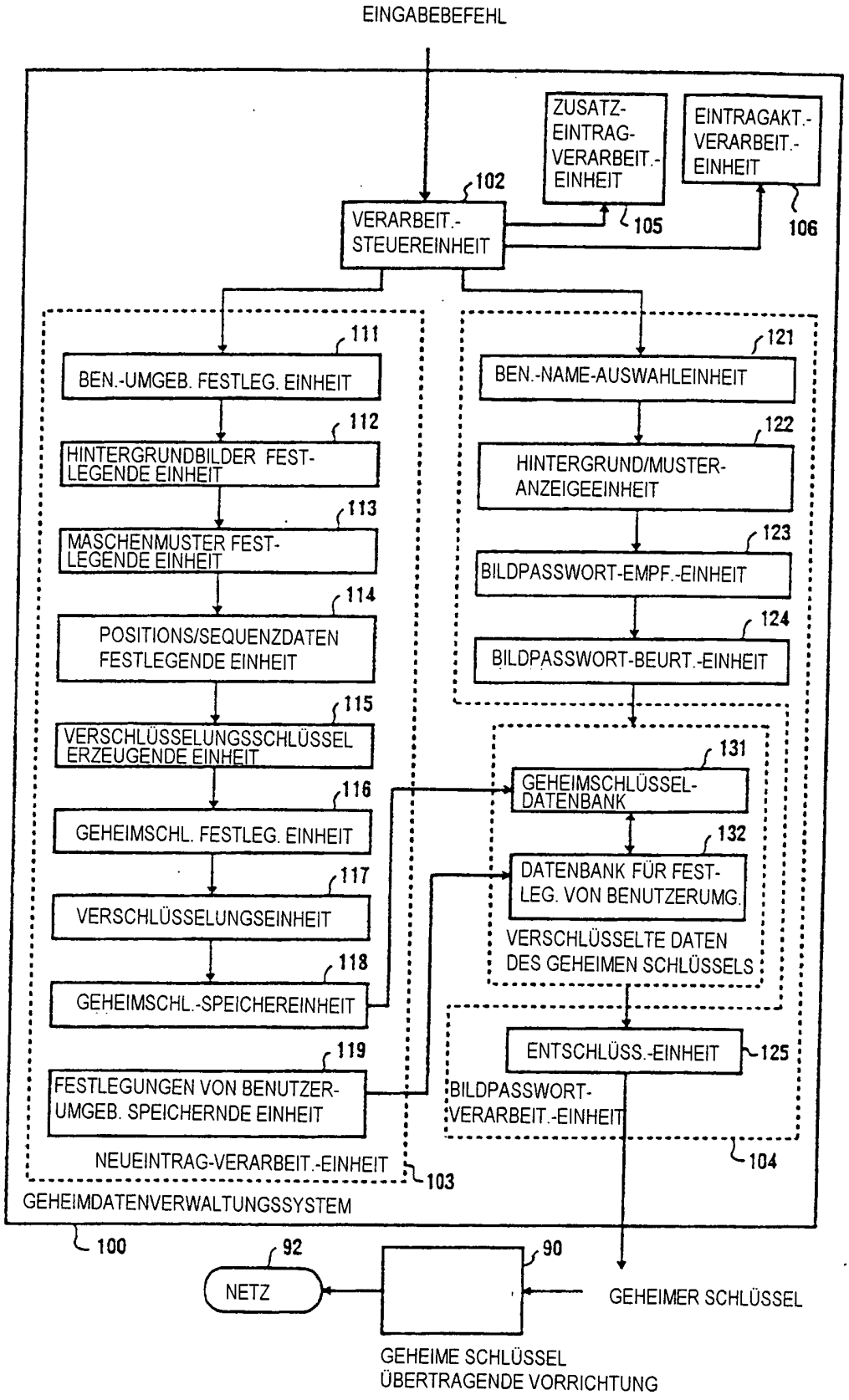

EINGABEBEFEHL
ZUSATZ-EINTRAG-VERARBEIT.-EINHEIT
EINTRAGAKT.-VERARBEIT.-EINHEIT
102
VERARBEIT.-STEUEREINHEIT
105
106
111
BEN.-UMGEB. FESTLEG. EINHEIT
112
HINTERGRUNDBILDER FEST-LEGENDE EINHEIT
113
MASCHENMUSTER FEST-LEGENDE EINHEIT
114
POSITIONS/SEQUENZDATEN FESTLEGENDE EINHEIT
115
VERSCHLÜSSELUNGSSCHLÜSSEL ERZEUGENDE EINHEIT
116
GEHEIMSCHL. FESTLEG. EINHEIT
117
VERSCHLÜSSELUNGSEINHEIT
118
GEHEIMSCHL.-SPEICHEREINHEIT
119
FESTLEGUNGEN VON BENUTZER-UMGEB. SPEICHERNDE EINHEIT
NEUEINTRAG-VERARBEIT.-EINHEIT
103
121
BEN.-NAME-AUSWAHLEINHEIT
122
HINTERGRUND/MUSTER-ANZEIGEEINHEIT
123
BILDPASSWORT-EMPF.-EINHEIT
124
BILDPASSWORT-BEURT.-EINHEIT
131
GEHEIMSCHLÜSSEL-DATENBANK
132
DATENBANK FÜR FEST-LEG. VON BENUTZERUMG.
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS
ENTSCHLÜSS.-EINHEIT
125
BILDPASSWORT-VERARBEIT.-EINHEIT
104
GEHEIMDATENVERWALTUNGSSYSTEM
100
92
NETZ
90
GEHEIMER SCHLÜSSEL
GEHEIME SCHLÜSSEL ÜBERTRAGENDE VORRICHTUNG

FIG. 6

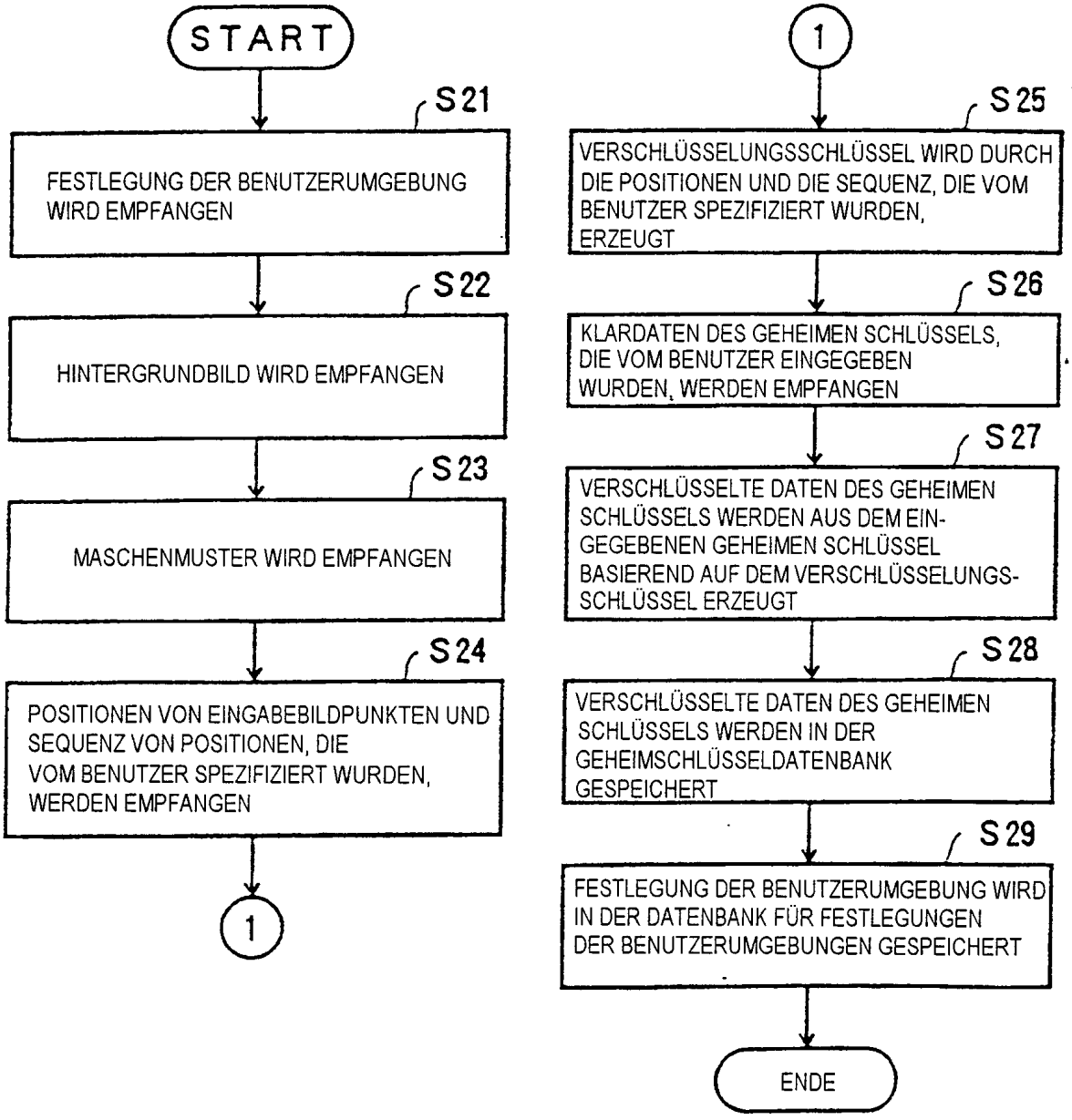

START
S21
FESTLEGUNG DER BENUTZERUMGEBUNG WIRD EMPFANGEN
S22
HINTERGRUNDBILD WIRD EMPFANGEN
S23
MASCHENMUSTER WIRD EMPFANGEN
S24
POSITIONEN VON EINGABEBILDPUNKTEN UND SEQUENZ VON POSITIONEN, DIE VOM BENUTZER SPEZIFIZIERT WURDEN, WERDEN EMPFANGEN
1
1
S25
VERSCHLÜSSELUNGSSCHLÜSSEL WIRD DURCH DIE POSITIONEN UND DIE SEQUENZ, DIE VOM BENUTZER SPEZIFIZIERT WURDEN, ERZEUGT
S26
KLARDATEN DES GEHEIMEN SCHLÜSSELS, DIE VOM BENUTZER EINGEGEBEN WURDEN, WERDEN EMPFANGEN
S27
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN AUS DEM EINGEGEBENEN GEHEIMEN SCHLÜSSEL BASIEREND AUF DEM VERSCHLÜSSELUNGSSCHLÜSSEL ERZEUGT
S28
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN IN DER GEHEIMSCHLÜSSELDATENBANK GESPEICHERT
S29
FESTLEGUNG DER BENUTZERUMGEBUNG WIRD IN DER DATENBANK FÜR FESTLEGUNGEN DER BENUTZERUMGEBUNGEN GESPEICHERT
ENDE

FIG. 7A

BENUTZER-CODE	CHIFFRE-CODE	GEHEIM-SCHLÜSSEL A	FRÜHERER ZUGRIFFSCODE	. . .

FIG. 7B

BENUTZER-CODE	BENUTZER-NAME	HINTERGRUND-BILDCODE	BENUTZER-UMGEBUNGS-CODE	. . .

FIG. 8

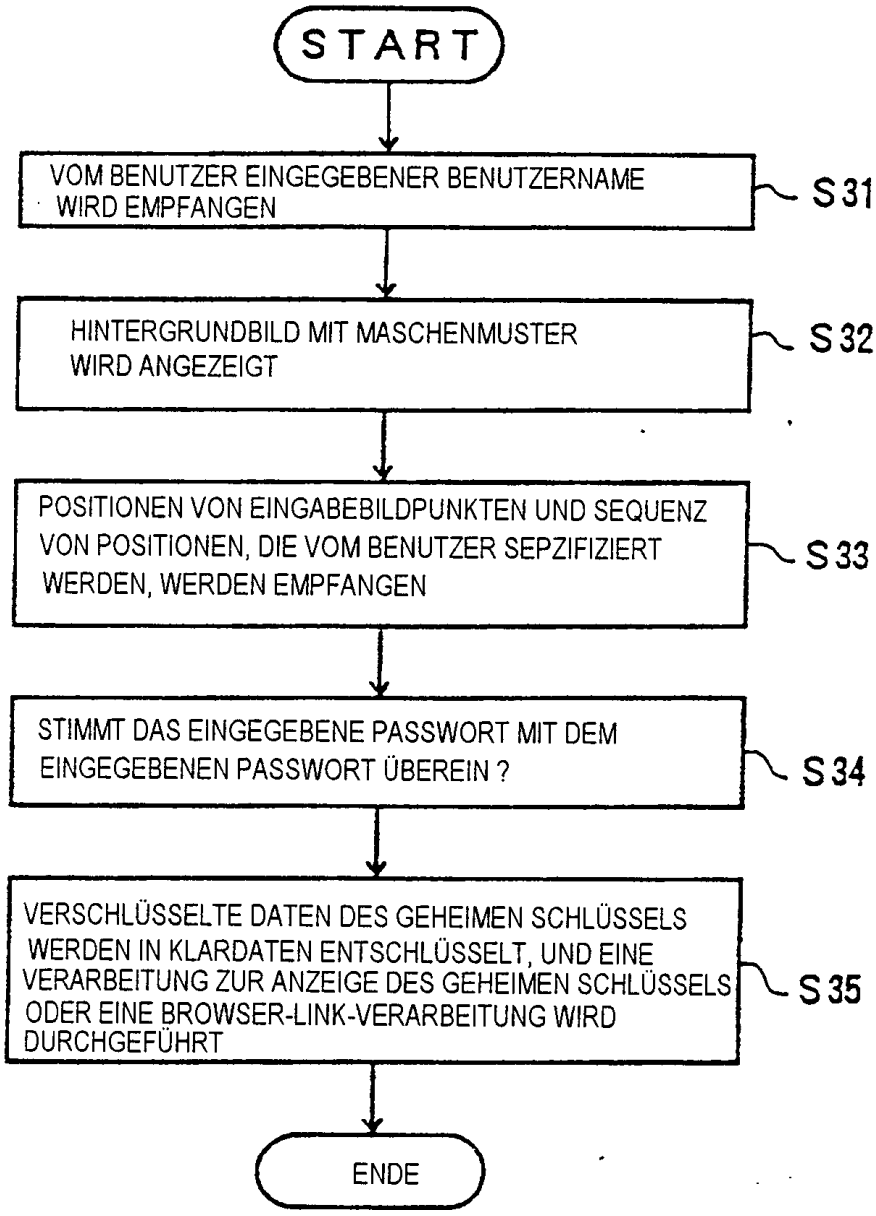

START
VOM BENUTZER EINGEGEBENER BENUTZERNAME WIRD EMPFANGEN
S31
HINTERGRUNDBILD MIT MASCHENMUSTER WIRD ANGEZEIGT
S32
POSITIONEN VON EINGABEBILDPUNKTEN UND SEQUENZ VON POSITIONEN, DIE VOM BENUTZER SEPZIFIZIERT WERDEN, WERDEN EMPFANGEN
S33
STIMMT DAS EINGEGEBENE PASSWORT MIT DEM EINGEGEBENEN PASSWORT ÜBEREIN ?
S34
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN IN KLARDATEN ENTSCHLÜSSELT, UND EINE VERARBEITUNG ZUR ANZEIGE DES GEHEIMEN SCHLÜSSELS ODER EINE BROWSER-LINK-VERARBEITUNG WIRD DURCHGEFÜHRT
S35
ENDE

FIG. 9

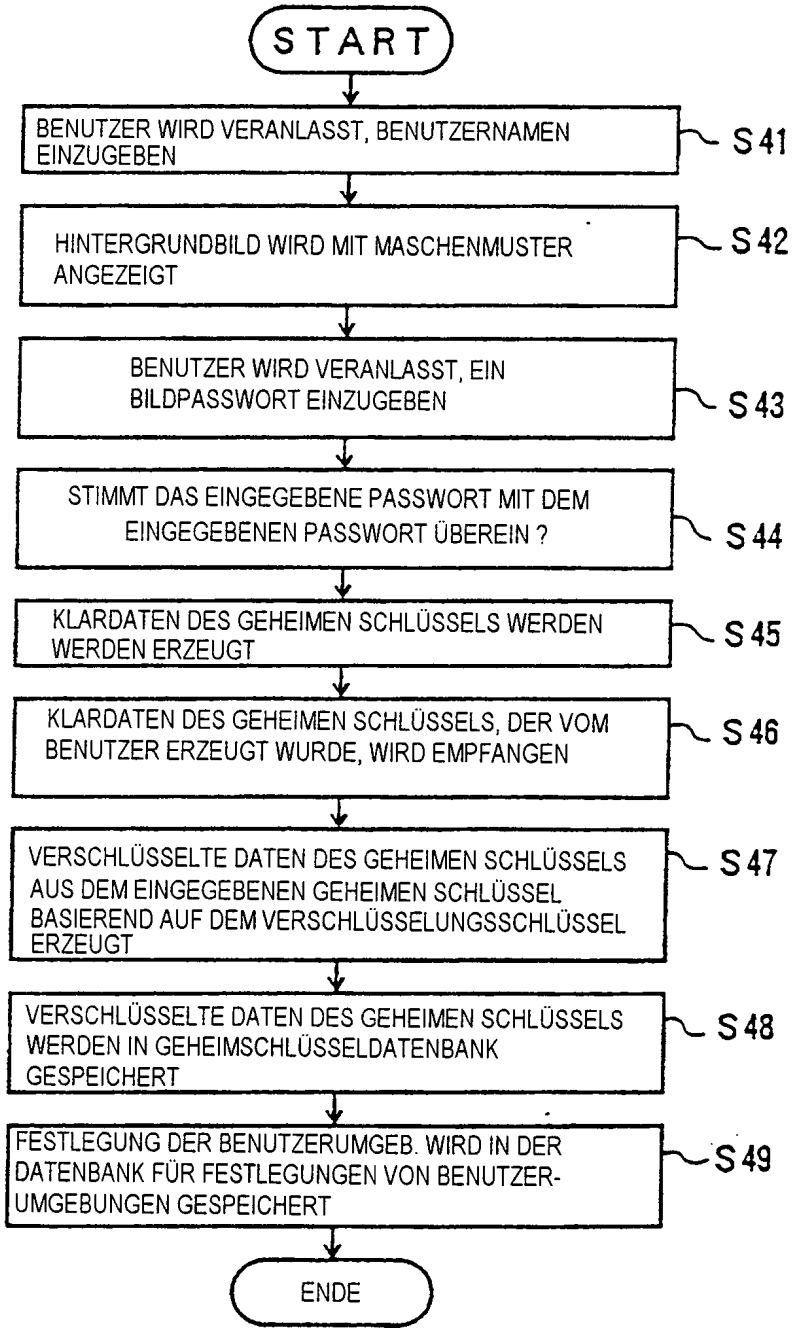
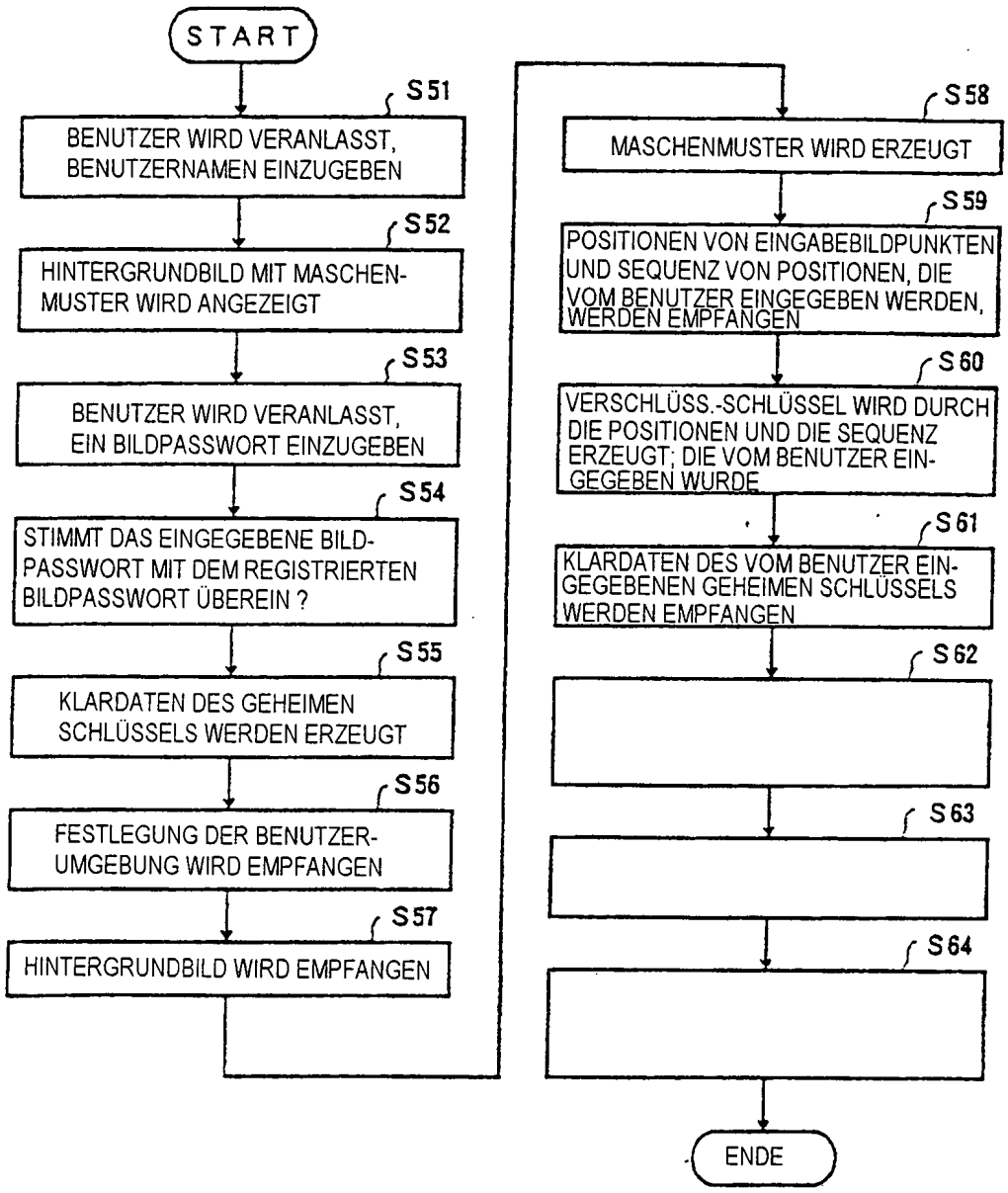

START
BENUTZER WIRD VERANLASST, BENUTZERNAMEN EINZUGEBEN
S41
HINTERGRUNDBILD WIRD MIT MASCHENMUSTER ANGEZEIGT
S42
BENUTZER WIRD VERANLASST, EIN BILDPASSWORT EINZUGEBEN
S43
STIMMT DAS EINGEGEBENE PASSWORT MIT DEM EINGEGEBENEN PASSWORT ÜBEREIN ?
S44
KLARDATEN DES GEHEIMEN SCHLÜSSELS WERDEN WERDEN ERZEUGT
S45
KLARDATEN DES GEHEIMEN SCHLÜSSELS, DER VOM BENUTZER ERZEUGT WURDE, WIRD EMPFANGEN
S46
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS AUS DEM EINGEGEBENEN GEHEIMEN SCHLÜSSEL BASIEREND AUF DEM VERSCHLÜSSELUNGSSCHLÜSSEL ERZEUGT
S47
VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN IN GEHEIMSCHLÜSSELDATENBANK GESPEICHERT
S48
FESTLEGUNG DER BENUTZERUMGEB. WIRD IN DER DATENBANK FÜR FESTLEGUNGEN VON BENUTZER-UMGEBUNGEN GESPEICHERT
S49
ENDE

FIG. 10

BENUTZER-CODE	CHIFFRE-CODE	GEHEIM-SCHLÜSSEL A	FRÜHERE ZUGRIFFS-ADRESSE	. . .
		GEHEIM-SCHLÜSSEL B	FRÜHERE ZUGRIFFS-ADRESSE	

FIG. 11



S62: VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN AUS DEM AUF DEM VERSCHLÜSSELUNGSSCHLÜSSEL BASIERENDEN EINGEGEBENEN GEHEIMEN SCHLÜSSEL ERZEUGT

S63: VERSCHLÜSSELTE DATEN DES GEHEIMEN SCHLÜSSELS WERDEN IN DER GEHEIMSCHLÜSSELDATENBANK GESPEICHERT

S64: FESTLEGUNG DER BENUTZERUMGEBUNG WIRD IN DER DATENBANK FÜR FESTLEGUNGEN VON BENUTZERUMGEBUNGEN GESPEICHERT

FIG. 12

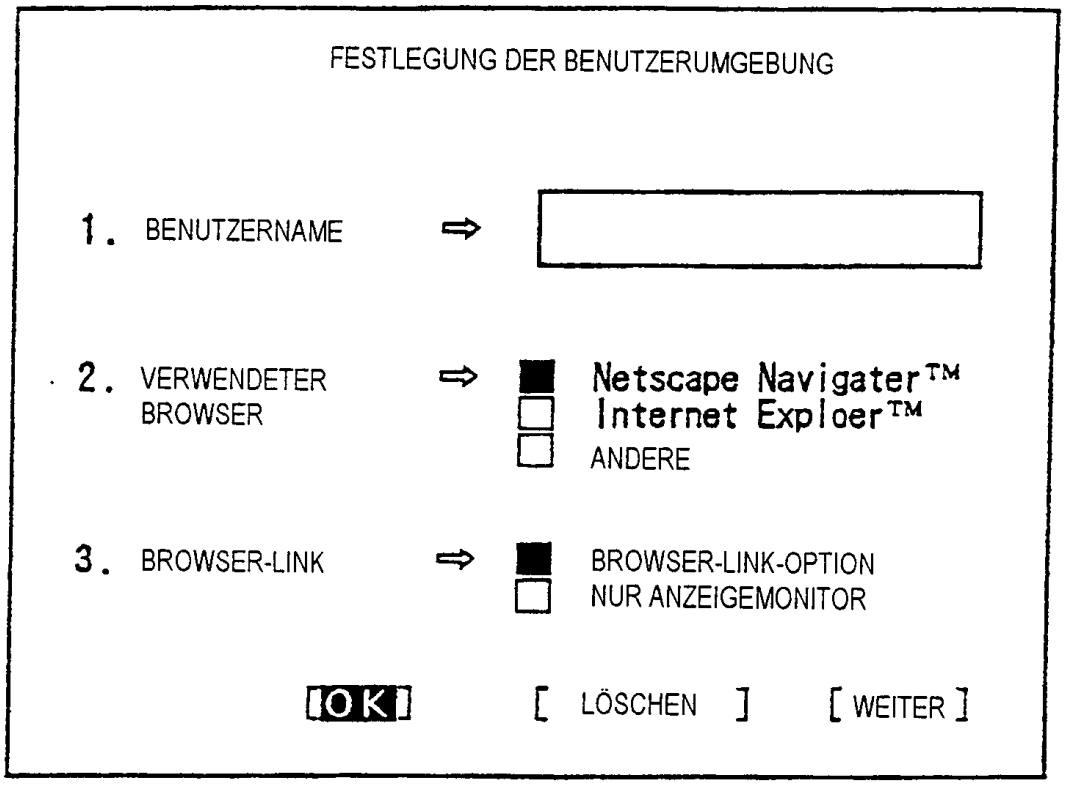

FESTLEGUNG DER BENUTZERUMGEBUNG
1. BENUTZERNAME
2. VERWENDETER BROWSER
Netscape Navigater™
Internet Exploer™
ANDERE
3. BROWSER-LINK
BROWSER-LINK-OPTION
NUR ANZEIGEMONITOR
[OK]
[LÖSCHEN]
[WEITER]

FIG. 13

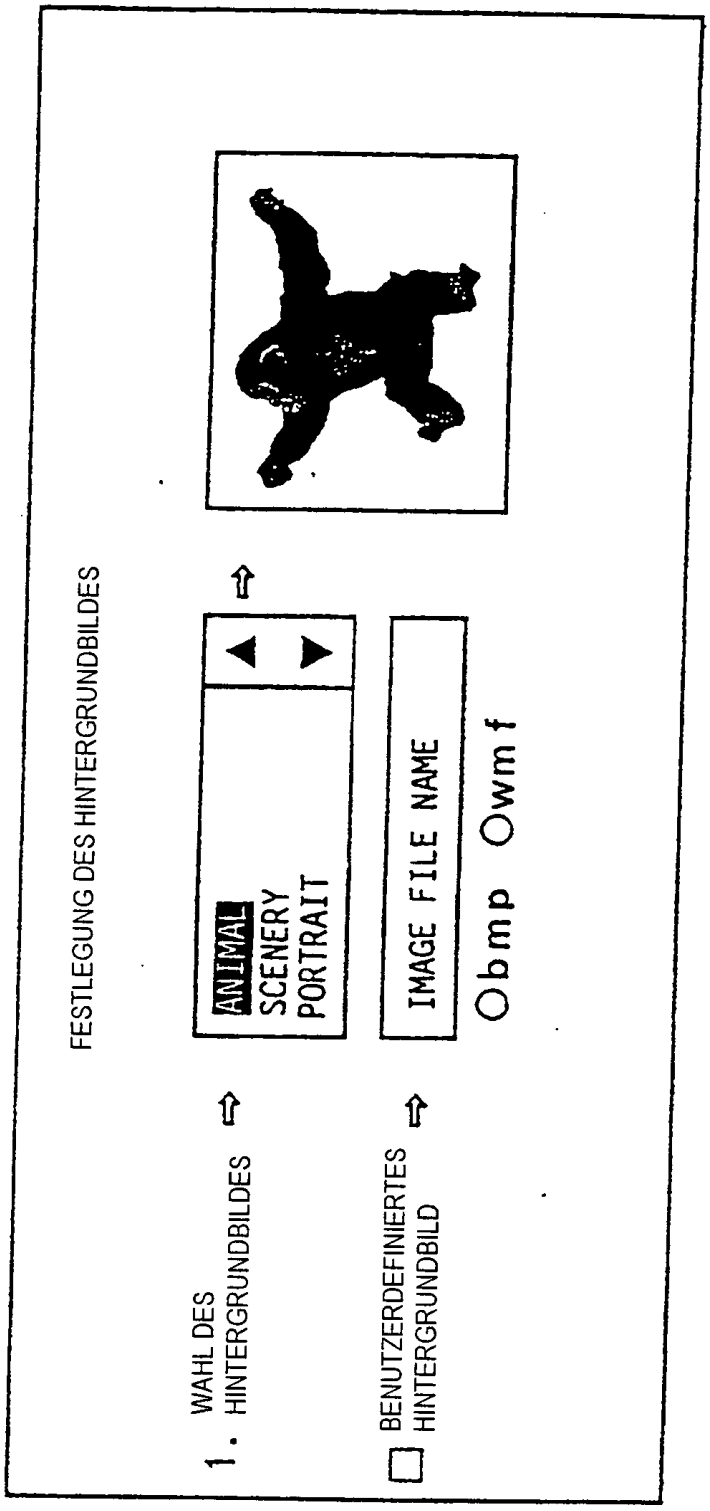

FESTLEGUNG DES HINTERGRUNDBILDES
1. WAHL DES HINTERGRUNDBILDES
ANIMAL
SCENERY
PORTRAIT
BENUTZERDEFINIERTES HINTERGRUNDBILD
IMAGE FILE NAME
bmp wmf

FIG. 14

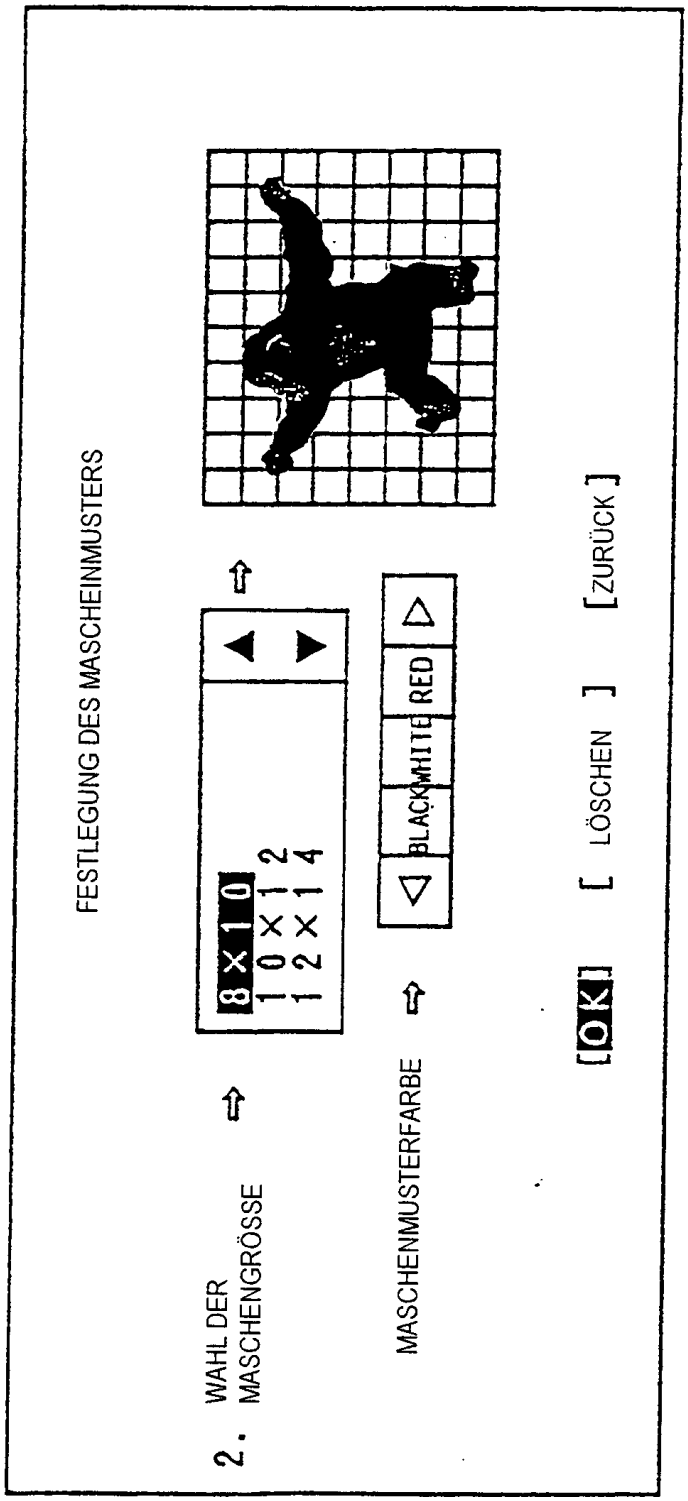

FESTLEGUNG DES MASCHEINMUSTERS
2. WAHL DER MASCHENGRÖSSE
8 X 1 0
1 0 X 1 2
1 2 X 1 4
MASCHENMUSTERFARBE
BLACK
WHITE
RED
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 15

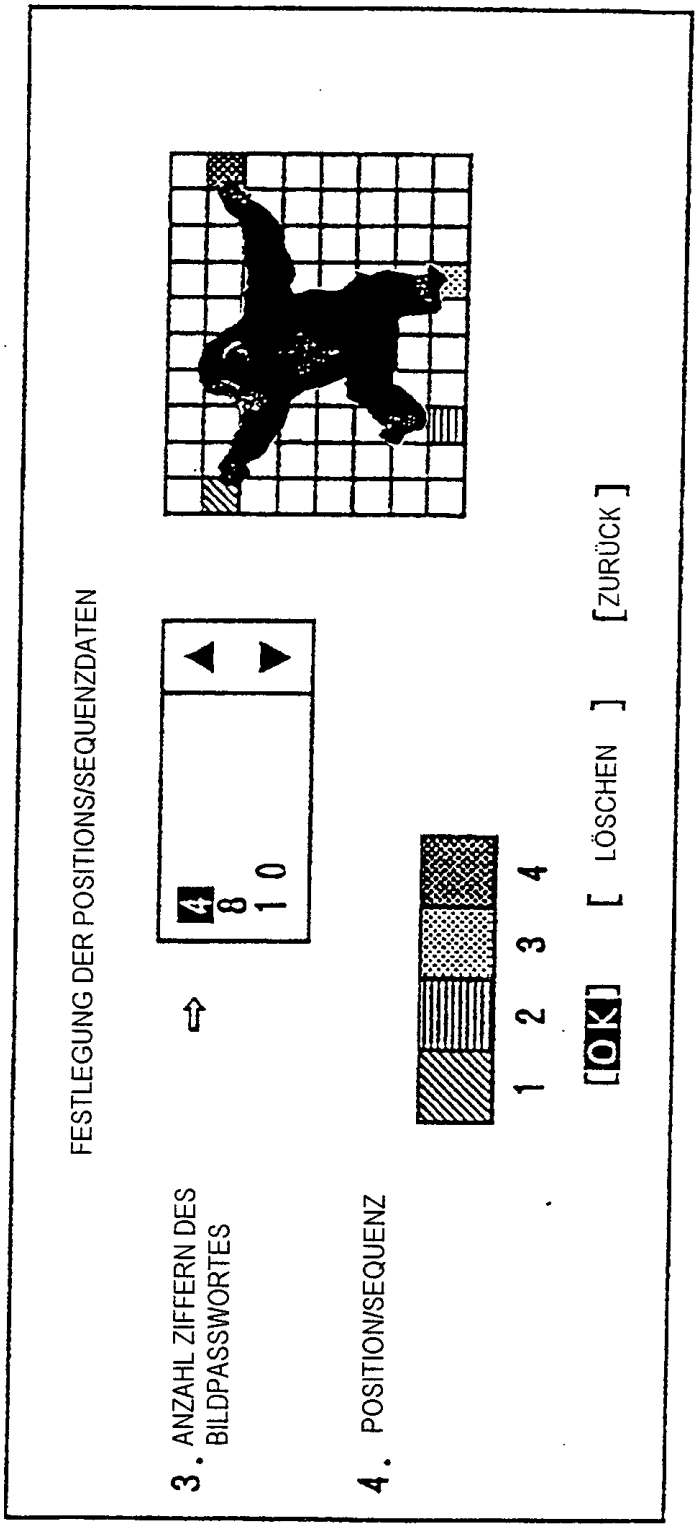

FESTLEGUNG DER POSITIONS/SEQUENZDATEN
3. ANZAHL ZIFFERN DES BILDPASSWORTES
4
8
10
4. POSITION/SEQUENZ
1 2 3 4
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 16

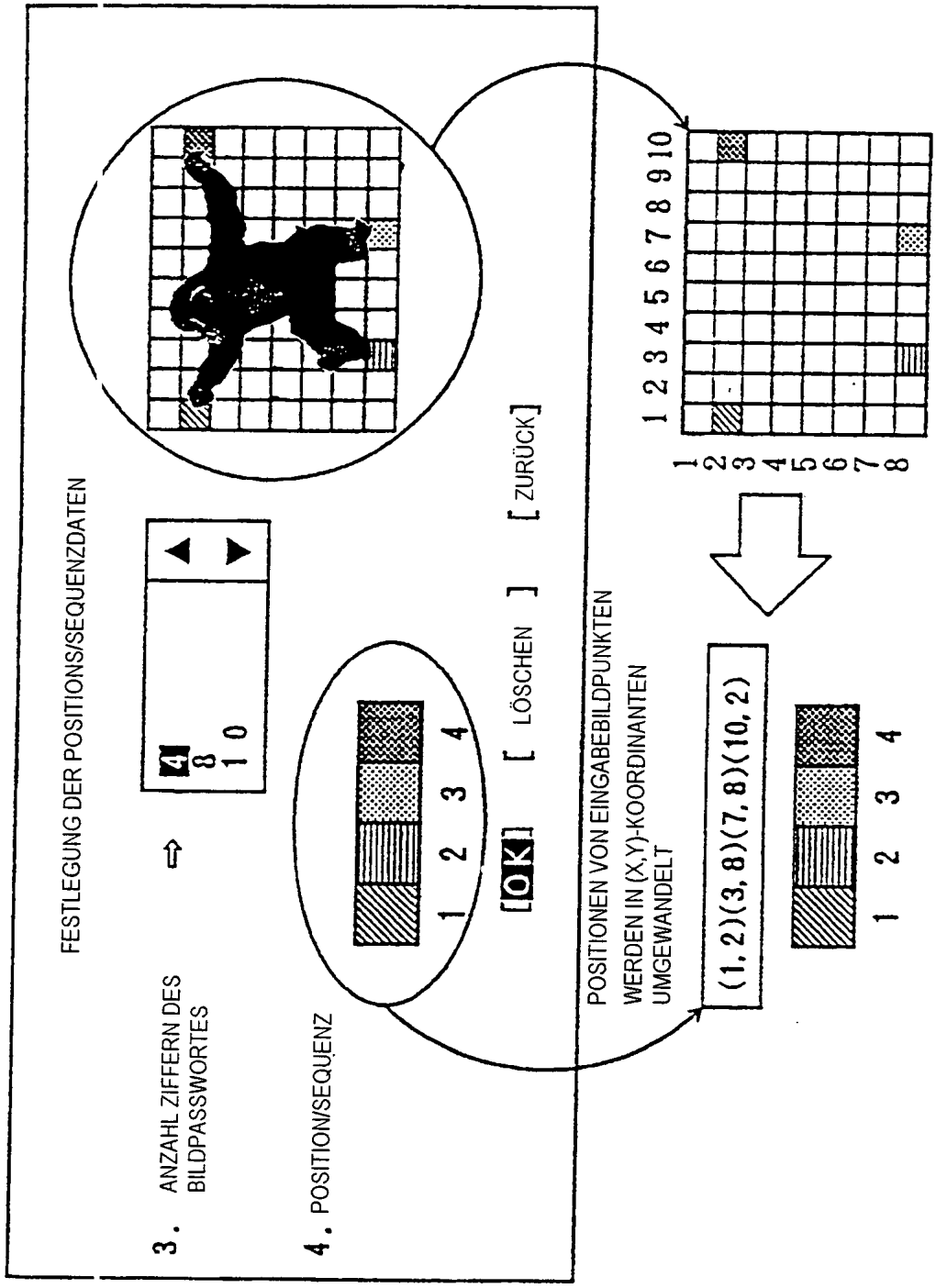

FESTLEGUNG DER POSITIONS/SEQUENZDATEN
3. ANZAHL ZIFFERN DES BILDPASSWORTES
4
8
10
4. POSITION/SEQUENZ
1 2 3 4
[OK]
[LÖSCHEN]
[ZURÜCK]
POSITIONEN VON EINGABEBILDPUNKTEN WERDEN IN (X,Y)-KOORDINANTEN UMGEWANDELT
(1, 2)(3, 8)(7, 8)(10, 2)
1 2 3 4 5 6 7 8 9 10
1 2 3 4 5 6 7 8
1 2 3 4

FIG. 17

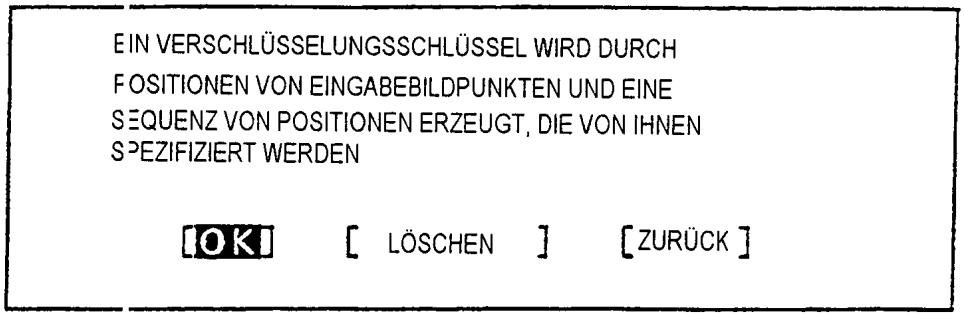

EIN VERSCHLÜSSELUNGSSCHLÜSSEL WIRD DURCH
POSITIONEN VON EINGABEBILDPUNKTEN UND EINE
SEQUENZ VON POSITIONEN ERZEUGT, DIE VON IHNEN
SPEZIFIZIERT WERDEN
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 18

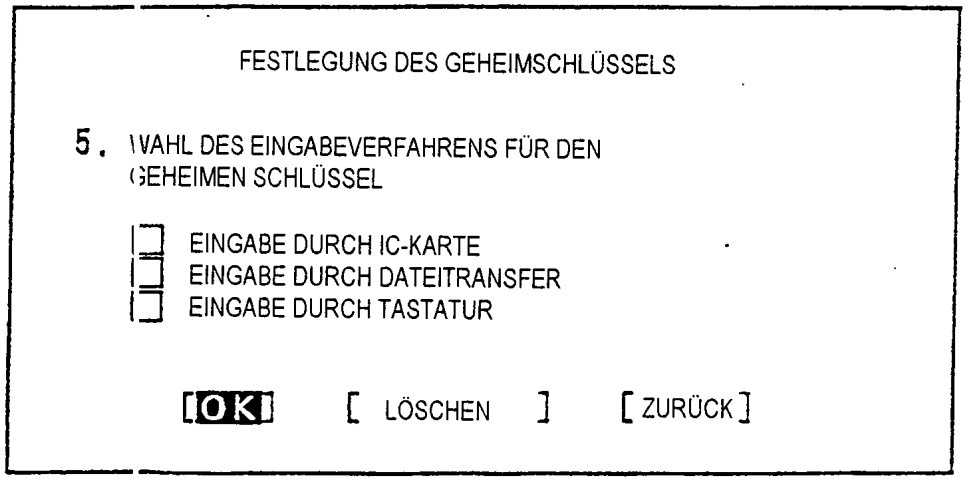

FESTLEGUNG DES GEHEIMSCHLÜSSELS
5. WAHL DES EINGABEVERFAHRENS FÜR DEN
GEHEIMEN SCHLÜSSEL
EINGABE DURCH IC-KARTE
EINGABE DURCH DATEITRANSFER
EINGABE DURCH TASTATUR
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 19

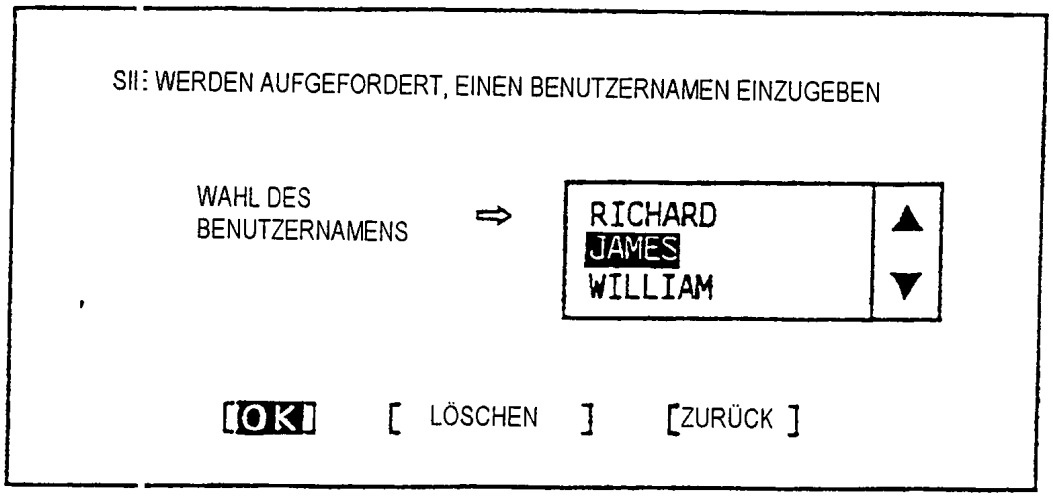

SIE WERDEN AUFGEFORDERT, EINEN BENUTZERNAMEN EINZUGEBEN
WAHL DES BENUTZERNAMENS
RICHARD
JAMES
WILLIAM
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 20

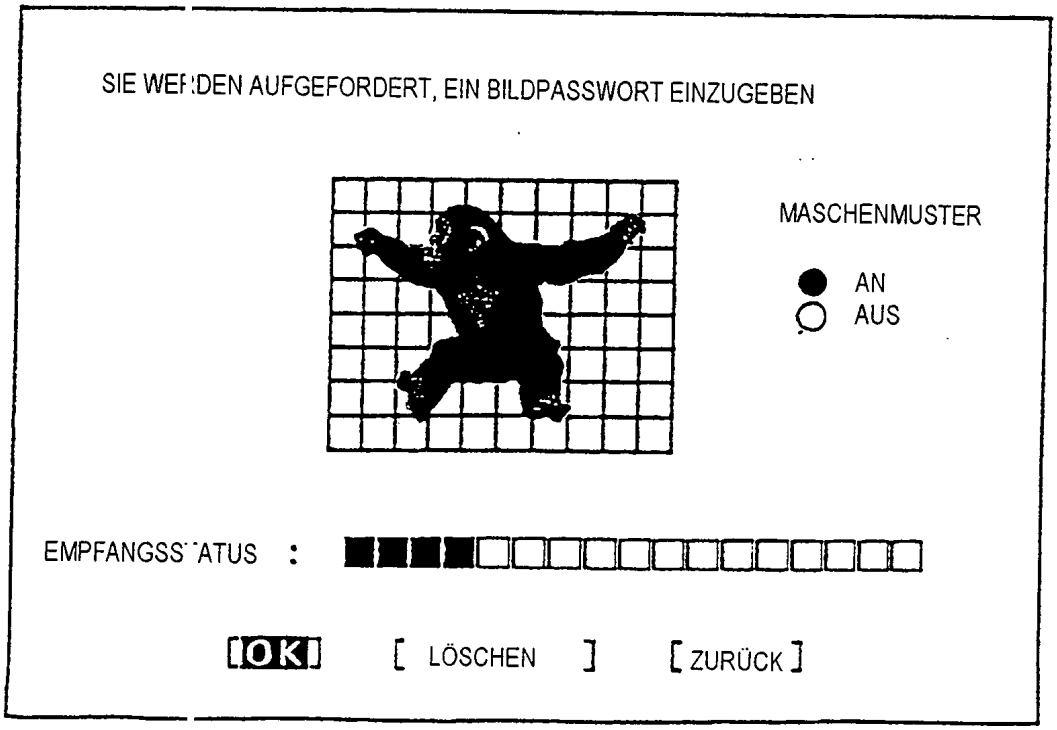

SIE WERDEN AUFGEFORDERT, EIN BILDPASSWORT EINZUGEBEN
MASCHENMUSTER
AN
AUS
EMPFANGSSTATUS :
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 21

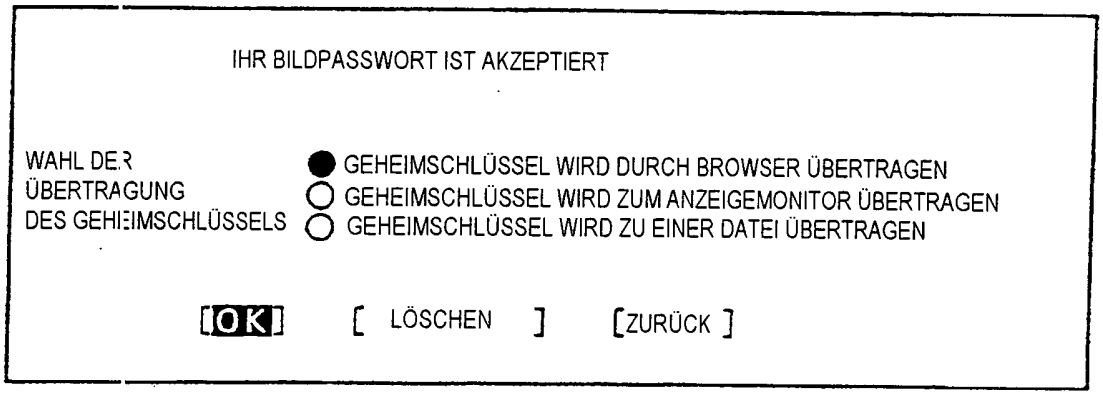

IHR BILDPASSWORT IST AKZEPTIERT
WAHL DER ÜBERTRAGUNG DES GEHEIMSCHLÜSSELS
GEHEIMSCHLÜSSEL WIRD DURCH BROWSER ÜBERTRAGEN
GEHEIMSCHLÜSSEL WIRD ZUM ANZEIGEMONITOR ÜBERTRAGEN
GEHEIMSCHLÜSSEL WIRD ZU EINER DATEI ÜBERTRAGEN
[OK]
[LÖSCHEN]
[ZURÜCK]

FIG. 22A

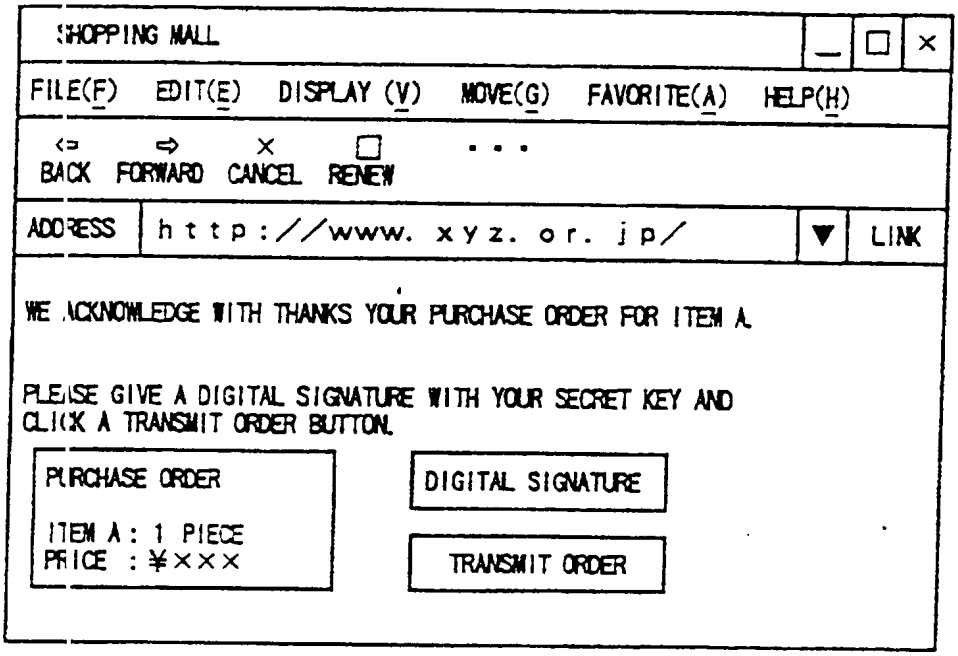


FIG. 22B

