(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
30. Oktober 2008 (30.10.2008)

(10) Internationale Veröffentlichungsnummer
WO 2008/128528 A2

(51) Internationale Patentklassifikation:
G09C 5/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/DE2008/000688

(22) Internationales Anmeldedatum:
19. April 2008 (19.04.2008)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2007 018 802.3 20. April 2007 (20.04.2007) DE

(71) Anmelder und
(72) Erfinder: **BORCHERT, Bernd** [DE/DE]; Ludwig-Schriever-Str. 16, 48480 Lüne (DE). **REINHARDT, Klaus** [DE/DE]; Weissdomweg 14, 72076 Tübigen (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*
— *hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii)*
— *Erfindererklärung (Regel 4.17 Ziffer iv)*

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

(54) **Title:** ANTI-TAPPING AND MANIPULATION ENCODING FOR ONLINE ACCOUNTS

(54) **Bezeichnung:** ABHÖR- UND MANIPULATIONSSICHERE VERSCHLÜSSELUNG FÜR ONLINE-ACCOUNTS

(57) **Abstract:** The invention relates to a method for anti-tapping and manipulation encoding for online accounts, in particular for online banking, by means of visual cryptography. A first partial secret image is generated on a film by the server according to the method of visual cryptography. A second partial secret image is generated by the server with keypads with random characters and displayed on the screen of the client, the keypad being clickable with the mouse. In the next step, the film and the screen are superimposed by the client such that both partial secret images give the image with the clickable keypad with written characters. The client can now enter a sequence of n characters by n mouse clicks on the keypads with characters. The information about which keys the client has clicked in which sequence is then transmitted to the server and the inputted sequence of characters reconstructed in the server.

(57) **Zusammenfassung:** Die vorliegende Erfindung betrifft ein Verfahren zur abhör- und manipulationssicheren Verschlüsselung für Online-Accounts, insbesondere für Online-Banking, mittels Visueller Kryptographie. Hierzu wird ein erstes Teilgeheimnis-Bild gemäß dem Verfahren der Visuellen Kryptographie auf einer Folie durch den Server erzeugt. Ferner wird ein zweites Teilgeheimnis-Bild mit Schaltflächen, die nach dem Zufallsprinzip mit Zeichen beschriftet werden, durch den Server erzeugt und auf dem Bildschirm des Klienten angezeigt, wobei die Schaltflächen durch die Maus anklickbar sind. Im nächsten Schritt werden die Folie und der Bildschirm vom Klienten so übereinander gelegt, dass die beiden Teilgeheimnis-Bilder das Bild mit den anklickbaren und mit Zeichen beschrifteten Schaltflächen ergeben. Der Klient kann nun einer Reihe von n Zeichen via n Mausklicks auf die beschrifteten Schaltflächen eingeben. Die Information darüber, welche Schaltflächen der Klient in welcher Reihenfolge angeklickt hat, wird dann zum Server übertragen und dort die eingegebene Zeichenreihe rekonstruiert.

WO 2008/128528 A2

Borchert1

Anmelder:
Bernd Borchert
Ludwig-Schriever-Str. 16
D-48480 Lünne

Abhör- und manipulationssichere Verschlüsselung für Online-Accounts

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zur abhör- und manipulationssicheren Verschlüsselung für Online-Accounts, insbesondere für Online-Bankkonten, mittels Visueller Kryptographie.

Die Abhör- und Manipulations-Sicherheit von Online-Accounts - insbesondere die von Online-Bankkonten - wird durch die immer größer werdende Quantität und Schädlichkeit von Malware (d.h. Viren etc.) auf den PC's der Bankkunden gefährdet. Verfahren, die sowohl das Abhören der PIN als auch einen sogenannten Man-in-the-Middle-Angriff sicher verhindern, sind technisch aufwändig und benötigen spezielle Hard- und Software auf dem vom Bankkunden benutzten PC.

Die Abhörbarkeit der PIN ist beim PIN/TAN Verfahren offensichtlich: die Malware auf dem Rechner des Klienten beobachtet heimlich beim Eingeben der PIN die Tastatureingabe. Später wird die abgehörte PIN heimlich per Rechnernetz an einen anderen Rechner weitergegeben. Von dort aus kann dann zumindest lesend auf den Account zugegriffen werden. Verfahren, bei denen die PIN mit Maus-Klicks auf den Bildschirm eingegeben wird, sind ebenfalls nicht abhörsicher: die Malware hört gleichzeitig Bildschirm und Mausbewegung ab.

Verfahren wie HBCI-2 für Bankkonten (mit externem Nummerfeld zur Eingabe der PIN) oder die Uhr-gesteuerten Security Tokens für Unternehmens-Accounts sichern die PIN vor dem Abhören ab, sind aber aufwändig in Herstellung und Benutzung.

Der sogenannte Man-in-the-Middle Angriff auf einen Online-Account sieht folgendermaßen aus: Bankkunde X möchte 50 Euro auf das Konto von Y überweisen. Er füllt das entsprechende Online Formular aus und schickt es ab. Die Malware auf dem Rechner fängt diesen Überweisungsauftrag ab, bevor er an die Bank geschickt wird, wandelt ihn in eine Überweisung von 5000 Euro an Z um, und schickt diesen manipulierten Überweisungsauftrag an die Bank. Die Nachfrage der Bank an X nach einer TAN für den Überweisungsauftrag von 5000 Euro an Z wird von der Malware in der umgekehrten Richtung ebenfalls abgefangen, und es wird dem Bankkunden X am Bildschirm die Nachfrage der Bank nach einer TAN für einen Überweisungsauftrag von 50 Euro an Y vorgespiegelt. Ahnungslos bestätigt X mit einer TAN diesen vorgespiegelten Auftrag, und die Malware schickt die von X eingegebene TAN an die Bank weiter, um den betrügerischen Überweisungsauftrag von 5000 Euro an Z zu bestätigen.

Die Verfahren PIN/TAN, PIN/iTAN, HBCI-1, HBCI-2, und Security Token schützen nicht sicher vor dem Man-in-the-Middle Angriff. Auch die Verschlüsselung der Verbindung (z.B. SSL) schützt nicht sicher, denn die Malware kann sich schon vor Beginn der Verbindungs-Verschlüsselung einschalten und die Manipulationen noch vor der Verbindungs-Verschlüsselung (bzw. in der anderen Richtung: nach der Verbindungs-Entschlüsselung) durchführen.

Verfahren, die sicher vor dem Man-in-the-Middle-Angriff schützen, sind die, die sowohl eine Ziffern-Tastatur als auch eine Anzeige außerhalb des Klienten Rechners anbringen, wie z.B. HBCI-3. Allerdings besteht wegen der physikalisch bestehenden Kabelverbindung zwischen dieser Extra-Hardware und dem

Rechner des Klienten immer noch ein Restrisiko, dass Malware auf dem Rechner des Klienten die Aktionen auf der Extra-Hardware ausspioniert. Eine weitere Möglichkeit ist es, sich die Überweisungsdaten per SMS von der Bank bestätigen zu lassen („mTANs"). Nachteilig an dieser Lösung ist, dass ein Handy vorhanden sein muss und dass der Empfang der SMS eventuell eine Weile dauert. Außerdem ist es nur eine Frage der Zeit, bis auch Handys von Malware befallen werden und damit diese Möglichkeit auch unsicher wird.

Einige der bekannten Verschlüsselungsverfahren basieren auf der Methode der Visuellen Kryptographie. Visuelle Kryptographie ist ein Verfahren, ein Schwarz-Weiß-Bild so in zwei Schwarz-Weiß-Bilder (Teilgeheimnis-Bilder) aufzuteilen, dass beide Teilgeheimnis-Bilder einzeln keine Information haben, aber wenn eins der beiden Teilgeheimnis-Bilder auf durchsichtige Folie gedruckt wird und auf das andere gelegt wird, das Original-Bild wieder zu sehen ist (mit 50% Kontrastverlust: aus weiß wird grau) (Naor & Shamir "Visual Cryptography", Advances in Cryptology, EUROCRYPT, Springer Verlag, 1994, pp. 1-12; siehe **Abb. 1**). Dabei kann eins der beiden Teilgeheimnis-Bilder schon im Voraus erzeugt werden, d.h. ohne dass das Original-Bild bekannt ist. Das zweite Teilgeheimnis-Bild wird dann abhängig vom Original-Bild und dem ersten Teilgeheimnis-Bild erzeugt (dass dieses zweite Bild ein Rauschbild ist, d.h. keine Information enthält, also insbesondere nicht die Information des Original-Bildes enthält, ist überraschend, aber mathematisch leicht nachweisbar).

Die Patente EP1472584B1 und US2005/0219149A1 beschreiben eine Anwendung der Visuellen Kryptographie, bei der eine durchsichtige elektronische Anzeige auf dem Bildschirm befestigt wird. Ein großer Nachteil dieses Verfahrens liegt darin, dass die Entwicklungs- und Herstellungskosten für diese Technik sehr hoch sind.

Das Patent EP1487141A1 beschreibt die Möglichkeit, schon eins der beiden Teilgeheimnisbilder der Visuellen Kryptographie im Voraus anlegen und an den Empfänger verteilen zu können, auch wenn das zu verschlüsselnde Bild noch

nicht bekannt ist (diese Möglichkeit ist bei jedem One-Time-Pad Verfahren gegeben, also insbesondere auch bei Visueller Kryptographie). Das Verfahren gibt Anwendungen dieses Prinzips auf die sichere Übermittlung von Nachrichten an, aber nicht im Zusammenhang mit Online Accounts.

Das Patent US2006/0098841A1 beschreibt ein Verfahren, mit dem n Zeichen eines Alphabets mit m Zeichen mit n Maus-Klicks abhörsicher übertragen werden können. Das Verfahren benötigt n mal m viele Schaltflächen. Dadurch ergibt sich in der Praxis eine Anzahl von Schaltflächen, die nicht mehr anzeigbar ist (Beispiel: Textlänge n=20, Alphabetgröße m=50 ergibt 1000 Schaltflächen).

Das Patent US20060020559A1 beschreibt ein Verschlüsselungsverfahren für Online-Accounts. Bei diesem Verfahren werden ausgestanzte Papierkarten auf den Bildschirm gelegt, um dem Benutzer eine geheime Information zu zeigen (dieses Prinzip ist auch als „Richelieu-Brett" bekannt). Das Verfahren hat u.a. den Nachteil, dass der Abhörsicherheit wegen große Teile der Karte undurchsichtig sein müssen und deshalb die Maus nicht mitverfolgt werden kann. Ein weiterer Nachteil dieses Verfahrens ist, dass bei einem Einsatz gegen den Man-in-the-Middle Angriff die ausgestanzte Papierkarte sehr groß werden würde.

In dem Aufsatz (Naor & Pinkas "Visual Authentication and Identification", CRYPTO, Springer Verlag, 1997, pp. 322-336) wird die Anwendung von Visueller Kryptographie für die Sicherheit von Smartcards vorgeschlagen and analysiert.

Es ist bislang jedoch kein Verfahren bekannt, mit dem bei niedrigen Herstellungskosten die Online-Accounts absolut sicher vor Malware Eingriffen geschützt werden können.

Die Aufgabe der vorliegenden Erfindung ist es daher, ein sicheres Verschlüsselungsverfahren für Online-Accounts bereit zu stellen, bei dem die Entwicklung- und die Herstellungskosten im Vergleich zu bekannten Verfahren wesentlich niedriger liegen.

Zur Lösung dieser Aufgabe wird die Methode der Visuellen Kryptographie verwendet, wobei erfindungsgemäß das neue Prinzip „Folie-auf-Bildschirm" eingesetzt wird: das eine Teilgeheimnis-Bild wird auf eine durchsichtige Folie gedruckt, das andere wird am Bildschirm angezeigt. Beim Auflegen der Folie auf den Bildschirm ist also für den Benutzer die Original-Information zu sehen. Entscheidend ist, dass keine Malware auf dem Rechner des Benutzers oder im Rechnernetz die Original-Information erkennen kann: es gibt keine Möglichkeit für Malware, die Folie auf dem Bildschirm zu „scannen". **Abb. 4** zeigt die Situation: das Teilgeheimnis-Bild auf dem Bildschirm und das Teilgeheimnis-Bild auf der Folie des Benutzers lassen übereinandergelegt ein Nummernfeld mit nach dem Zufallsprinzip vertauschten Ziffern erkennen. Für Malware auf dem Rechner oder im Rechnernetz besteht keine Möglichkeit, die Vertauschung der 10 Ziffern zu erkennen.

Unter dem Begriff „Folie" wird hier und im Folgenden eine dünne Schicht aus einem geeigneten Material verstanden, die bedruckt oder ausgestanzt sein kann. Insbesondere kann hierzu ein im Wesentlichen transparentes Material wie Kunststoff oder durchsichtiges Papier verwendet werden, welches mit einem der Teilgeheimnis-Bilder bedruckt wird. Alternativ wird ein undurchsichtiges Material eingesetzt, welches zum Erzeugen eines Teilgeheimnis-Bildes erfindungsgemäß ausgestanzt wird. Besonders vorteilhaft eignet sich hierzu dunkles, z.B. schwarzes Papier, damit der optische Kontrast am größten ist.

Damit das auf der Folie aufgedruckte Teilgeheimnis-Bild mit dem auf dem Bildschirm angezeigten Teilgeheimnis-Bild passend übereinander gelegt werden kann, wird die Folie auf dem Bildschirm fixiert. Hierzu können einzelne Folien an einem oder an mehreren Rändern mit Klebestreifen versehen werden. In diesem Fall können die Folien analog zu Haftnotizen in einem Notizblock übereinander gestapelt und durch die Klebestreifen zusammengehalten aufbewahrt werden.

Es wird im Folgenden ein Beispiel des erfindungsgemäßen Verfahrens zur abhörsicheren Handhabung eines Online-Accounts beschrieben. In diesem Beispiel wird ein Text mit n Zeichen aus einem Alphabet bestehend aus m Zeichen mit n Maus-Klicks absolut abhörsicher von einem Klienten durch ein Rechnernetz zu einem Server übertragen. Hier und im Folgenden wird unter Alphabet, wie in der Informatik üblich, eine endliche Menge von Zeichen verstanden. In diesem Sinne ist zum Beispiel die Menge der Ziffern 0,...,9 ein Alphabet mit 10 Zeichen.

Zuerst erstellt der Server für jeden Klienten eine Menge von Teilgeheimnis-Bildern, die er mit Namen (z.B. Nummern) versieht und abspeichert. Dann druckt er diese Bilder auf durchsichtige Folien aus, druckt zusätzlich ihren jeweiligen Namen (Nummer) sichtbar darauf, und schickt diese Folien physikalisch, also z.B. per Post, an den Klienten. Anfangs haben alle diese Teilgeheimnis-Bilder den Status „unverbraucht", der später in „verbraucht" wechseln kann. Dieser Status wird vom Server verwaltet.

Der Klient X hat jetzt diese Folien und will dem Server eine geheime Nachricht von n Zeichen schicken (Beispiel: er will ihm eine 8-stellige Bankleitzahl übermitteln). Dazu tritt er auf seinem Rechner online über das Rechnernetz mit dem Server in Verbindung und stellt sich dort dem Server als Klient X vor.

Der Server nimmt Notiz davon und erzeugt dann ein Original-Bild zur Übertragung von n Zeichen aus einem Alphabet mit m Zeichen auf folgende Weise. Auf dem Bild werden mindestens n+m-1 Schaltflächen erzeugt. Die Schaltflächen dienen als Flächen zum späteren Anklicken durch die Maus und überlappen sich nicht. Die Schaltflächen tragen Beschriftungen. Jedes Zeichen des Alphabets erscheint als Beschriftung auf mindestens einer der Schaltflächen. Zusätzlich gibt es n-1 Schaltflächen, die jeweils für einen Verweis auf ein Zeichen stehen, das schon vorgekommen ist. Idealerweise sind diese Verweise mit den Positionen 1 bis n-1 nummeriert beschriftet (falls die Ziffern selber Bestandteil des Alphabets sind, werden diese Zahlen speziell gekennzeichnet,

z.B. durch ein vorangesetztes P für „Position"). **Abb. 2A** zeigt so ein Bild mit Schaltflächen für die Ziffern 0,...,9 und Textlänge n=8, **Abb. 2B** zeigt ein Bild für ein Alphabet mit den Buchstaben A...,Z, den Ziffern 0,..,9 plus ein paar Sonderzeichen, und Textlänge n=10. Die Zuordnung von Beschriftungen und Schaltflächen wird zufällig erzeugt. Der Server merkt sich diese zufällige Zuordnung.

Ein spezieller Fall liegt vor, wenn der zu übermittelnde Text garantiert keine Zeichen-Wiederholung hat (ein plausibles Beispiel: es werden nur PINs bestehend aus den Ziffern 0,...,9 erlaubt, in denen keine Ziffern mehrfach vorkommen). In diesem Fall können die Schaltflächen mit den Verweisen auf die vorherige Position wegfallen, und es reicht eine Schaltfläche für jedes Zeichen des Alphabets. **Abb. 2C** zeigt ein Bild mit einer zufällig erzeugten Anordnung von Schaltflächen für die Ziffern 0,...,9.

Nachdem der Server ein solches Original-Bild erzeugt hat, nimmt er ein noch nicht verbrauchtes abgespeichertes Teilgeheimnis-Bild für den Klienten X, macht aus diesen beiden Bildern nach dem Verfahren der Visuellen Kryptographie ein zweites (elektronisches) Teilgeheimnis-Bild, welches er dann er durch das Rechnernetz online auf den Bildschirm des Klienten schickt. Ebenfalls wird der Name (Nummer) des abgespeicherten Teilgeheimnis-Bildes auf den Bildschirm des Klienten geschickt. Das abgespeicherte Teilgeheimnis-Bild bekommt beim Server den Status "verbraucht".

Der Klient X sieht das Teilgeheimnis-Bild und dessen Name (Nummer) auf dem Bildschirm, siehe **Abb. 3A**. Er legt die Folie mit dem gleichen Namen (Nummer) auf den Bildschirm, und zwar genau auf das Teilgeheimnis-Bild am Bildschirm. Weil die zwei Teilgeheimnis-Bilder nach dem Verfahren der Visuellen Kryptographie erzeugt wurden, kann der Klient X das Original-Bild sehen.

In der Praxis sind die beiden Bilder nicht gleich groß. Das Bild am Bildschirm muss also vom Klienten angepasst (z.B. gedehnt) werden können, am besten per Maus.

Der Klient sieht also das Original-Bild mit seinen Schaltflächen und deren Beschriftungen, siehe **Abb. 3B**. Er kann jetzt seinen geheimen Text via Maus-Klicks eingeben, und zwar nach folgenden Regeln.

Ein Text mit n oder weniger Zeichen wird folgendermaßen Zeichen für Zeichen eingegeben. Für jedes Zeichen, das vorher noch nicht vorgekommen ist, wird die Schaltfläche, auf dem das Zeichen steht, angeklickt. Falls ein Zeichen schon vorgekommen ist, wird die bisher größte Position im Text ermittelt, an der das Zeichen schon stand: die Schaltfläche, deren Beschriftung einen Verweis auf diese Position darstellt, wird angeklickt. Beispielsweise wird in **Abb. 3** die Bankleitzahl 20041111 durch Anklicken der folgenden Schaltflächen eingegeben: 2, 0, P2, 4, 1, P5, P6, P7.

Nach diesen einfachen Regeln ist es garantiert, dass jede Schaltfläche nur maximal einmal angeklickt wird. Die Software am Klienten-Rechner kann deswegen potentiell den Benutzer unterstützen und alle schon einmal anklickten Schaltflächen speziell anzeigen, z.B. im Teilgeheimnis-Bild auf dem Bildschirm alle Pixel der angeklickten Schaltfläche invertieren. So sieht der Benutzer, welche Schaltflächen er nicht mehr anklicken sollte, die Abhörsicherheit wird dadurch nicht beeinträchtigt.

Eine weitere mögliche Unterstützung für den Benutzer bieten – so wie er es vom Bank-Automaten kennt - eine Korrektur-Taste und eine Fortschrittsanzeige, die mit „Sternchen“ anzeigt, wie viele Zeichen schon eingegeben wurden.

An den Server wird die Information über die angeklickten Schaltflächen und deren Reihenfolge geschickt, z.B. indem die Pixel-Positionen der n Maus-Klicks relativ im Teilgeheimnis-Bild übermittelt werden, oder eine andere eindeutige

Beschreibung der angeklickten Schaltflächen übermittelt wird. Beispielsweise könnten die in **Abb. 3B** angeklickten Schaltflächen mit den Beschriftungen 2, 0, P2, 4, 1, P5, P6, P7 als Koordinaten der dargestellten 4x5 Matrix (mit (0,0) oben links und (3,4) unten rechts) übermittelt werden, also folgendermaßen: (3,2), (3,1), (0,0), (3,4), (1,0), (0,1), (3,0), (1,1).

Weil jede Schaltfläche maximal einmal angeklickt wird und die Beschriftung der Schaltflächen zufällig gewählt wurde, kann Malware auf dem Rechner des Klienten oder im Rechnernetz keinerlei Information über den übermittelten Text erschließen: die Malware müsste dazu die aufgelegte Folie ausspionieren, was nicht möglich ist.

Die an den Server geschickte Information kann dort anschließend entschlüsselt werden: der Server kennt das Originalbild und weiß, welche Beschriftungen die angeklickten Schaltflächen haben. Also kann er aus den übermittelten n Beschreibungen von Schaltflächen die vom Klienten eingegebene Nachricht von n Zeichen rekonstruieren. In dem Beispiel von oben, bei dem die Matrix-Koordinaten (3,2), (3,1), (0,0), (3,4), (1,0), (0,1), (3,0), (1,1) übermittelt wurden, kann der Server wegen der Kenntnis des Original-Bilds daraus direkt die Nachricht 20041111 herauslesen. Die Nachricht wurde also abhörsicher vom Klienten zum Server übertragen.

Umgekehrt kann auch ein geheimer Text vom Server an den Klienten geschickt werden: Der Server schreibt den Text auf ein Schwarz-Weiß-Bild, nimmt eine unverbrauchte Folie, und erzeugt aus beiden ein entsprechendes zweites, elektronisches Teilgeheimnis-Bild, welches er per Rechnernetz dem Klienten auf den Bildschirm schickt, einschließlich Name der Folie. Der Klient legt die entsprechende Folie auf den Bildschirm und kann den Text lesen. In dem Fall, dass der Klient überhaupt einen Text erkennen kann, weiß er sicher, dass der Text vom Server ist, denn niemand anders kennt seine Folie, und deshalb kann niemand eine Nachricht an ihn fälschen.

Der Bildschirm des Klienten kann erfindungsgemäß entweder ein Bildschirm eines Computers oder ein Bildschirm eines mobilen Endgeräts, insbesondere ein Display eines Handys, sein (**Abb. 7**).

Der Vorteil des beschriebenen Verfahrens liegt somit darin, dass ein Online Account sicher vor dem Abhören der PIN und sicher vor dem Man-in-the-Middle-Angriff geschützt werden kann. Der Grund liegt darin, dass Malware (auf dem Rechner des Bankkunden oder im Rechnernetz) die aufzulegende Folie nicht kennt und definitiv auch nicht ausspionieren kann (ein „Scannen" der Folie via Bildschirm ist absurd!).

Im Vergleich zum in US2006/0098841A1 beschriebenen Verfahren benötigt das erfindungsgemäße Verfahren nur n+m-1 Schaltflächen. Für das o.g. Beispiel (Textlänge n=20, Alphabetgröße m=50 ergibt 1000 Schaltflächen) heißt das: 69 Schaltflächen im vorliegenden Verfahren statt 1000, die im US2006/0098841A1 benötigt werden.

Ein weiterer Vorteil besteht in relativ niedrigen Herstellungskosten, da hierzu nur die entsprechenden Folien produziert und bedruckt werden müssen, keine teueren Vorrichtungen sind notwendig.

Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der Erfindung werden nachstehend anhand der Ausführungsbeispiele mit Bezug auf die Zeichnungen beschrieben. In den Zeichnungen zeigen:

Abb.1: Prinzip der Visuellen Kryptographie (Naor & Shamir): zwei Folien enthalten allein jeweils keine Information, übereinandergelegt geben sie jedoch eine Information preis.
(Hinweis: Die Abbildung Abb. 1 eignet sich zur Demonstration der Visuellen Kryptographie: Abb. 1 auf Folie kopieren, und dann das Bild oben auf das in der Mitte legen: man sieht dann das untere Bild.)

Abb. 2: drei Original-Bilder mit Schaltflächen zum Anklicken für die Maus.

Abb. 3: Abhörsichere Vermittlung von Information mit Wiederholung von Symbolen, Beispiel: Eingabe einer Bankleitzahl mit 8 Stellen.

Abb. 4: Abhörsichere Vermittlung von Information, bei der keine Wiederholungen von Symbolen auftreten, Beispiel: PIN-Eingabe (Annahme dabei: es werden nur PINs ohne Ziffern-Wiederholung vergeben)

Abb. 5: Fälschungssichere Bestätigung einer Überweisung inklusive Angabe einer TAN (die dann im Klartext auf der Tastatur eingegeben werden kann). Es ist für die Fälschungssicherheit wichtig, dass die Information nicht an einer festgelegten Stelle steht, z.B. sind in der Abbildung B die angezeigten Zahlen horizontal zufällig versetzt.

Abb. 6: Manipulationssichere online Bestätigung von Abbuchungen via Visueller Kryptographie.

Abb. 7: Manipulationssichere online Bestätigung von Abbuchungen via Visueller Kryptographie auf einem mobilen Endgerät.

Abb. 8: Abhörsichere Vermittlung von allgemeinem Text, inklusive Wiederholung von Zeichen.

Ausführungsbeispiel

Das oben angegebene Verfahren zum Senden geheimer Nachrichten zwischen Server und Klient wird angewandt auf den speziellen Fall des Online-Bankings (**Abb. 4** und **5**). Das Verfahren verhindert das Abhören der PIN und den Man-in-the-Middle Angriff.

Der Bank-Server erzeugt für den Bankkunden X eine Menge von Teilgeheimnis-Bildern, nummeriert sie, speichert sie ab, und schickt sie ausgedruckt auf Folien dem Bankkunden per Post zu (also so ähnlich wie TAN-Listen verschickt werden). Zusätzlich wird dem Kunden wie beim PIN/TAN Verfahren eine PIN zugestellt, dabei wird vorausgesetzt, dass in der PIN keine Ziffer doppelt vorkommt (die Anzahl der Möglichkeiten reicht immer noch, um ein Raten der PIN aussichtslos sein zu lassen)

Wenn der Kunde X die Folien und seine PIN empfangen hat, kann er mit dem Online Banking beginnen. Zum Einloggen geht er auf die Web-Seite der Bank und gibt dort seine Konto-Nr. an. Die Konto-Nr. wird an den Bank-Server geschickt. Der Bank-Server überprüft nun folgendermaßen die Authentizität von X:

Der Bank-Server erzeugt ein Original-Bild mit 10 Schaltflächen, z.B. in der Art, dass die Anordnung der Schaltflächen der Anordnung der Tasten des Nummernfelds auf einer Tastatur entspricht, siehe **Abb. 2C**. Zufällig werden die 10 Ziffern 0,...,9 auf diese Schaltflächen verteilt. Der Server merkt sich diese zufällige Vertauschung. Es wird eine unverbrauchte gespeicherte Folie für den Bankkunden X genommen und nach dem Verfahren der Visuellen Kryptographie wird aus ihr und dem Original-Bild ein zweites elektronisches Teilgeheimnis-Bild erzeugt. Dieses wird dem Bankkunden X in sein Browser-Fenster geschickt, einschließlich der Nummer des gespeicherten Teilgeheimnis-Bildes. Es entsteht die Situation wie in **Abb. 4A**.

Der Bankkunde sieht das Teilgeheimnis-Bild und dessen Nummer und legt seine entsprechende Folie darauf. Damit kann er das Nummernfeld erkennen, siehe **Abb. 4B**. Er klickt mit der Maus die entsprechenden Schaltflächen an. Angenommen, seine PIN sei 41629. Dann klickt er also in **Abb. 4B** nacheinander die Schaltflächen an, die auf dem normalen Nummerfeld die Ziffern 0, 5, 2, 9, 6 darstellen. Diese Ziffernfolge 05296 wird an den Bank-Server geschickt.

Der Bank-Server empfängt die Ziffernfolge 05296. Weil der Bank-Server selber das Original-Bild mir den vertauschten Ziffern erzeugt hat und sich die Vertauschung gemerkt hat, kann er daraus jetzt direkt schliessen, dass durch die Maus-Klicks die Ziffernfolge 41629 eingegeben wurde. Er vergleicht diese Ziffernfolge mit der PIN für Bankkunde X (die natürlich auch abgespeichert ist). Wenn das die richtige PIN war, bekommt der Bankkunde X Zugang zum Konto.

Lauschende Malware (auf dem Rechner, den der Bankkunde X benutzt, oder im Internet) hat keine Chance, die PIN abzuhören: die Positionen der Mausklicks und die zum Server geschickten Ziffernfolgen haben keine Bedeutung, solange nicht die Vertauschung der Ziffern auf dem Nummernfeld bekannt ist. Diese kennt aber nur der Bank-Server und derjenige, der am Browser die entsprechende Folie auflegen kann.

Bankkunde X bekommt also mit dem Wissen der PIN und dem physikalischen Besitz der Folie Zugang zu seinem Bank-Konto. Nur eins von beiden reicht nicht aus. Mit dem Verfahren wird die PIN also doppelt geschützt: erstens ist sie nicht abhörbar, und falls doch jemand auf andere Weise in ihren Besitz kommen sollte, braucht er die passende Folie: ohne sie kommt er nicht in den Account.

Im Folgenden wird dargestellt, wie das Verfahren einen Man-in-the-Middle Angriff vereitelt. Der Bankkunde X hat sich erfolgreich eingeloggt und möchte eine Überweisung von 50 Euro an Y vornehmen. Er tippt im Klartext in einem entsprechenden Formular Name, Konto-Nummer, BLZ und Betrag ein und schickt diese Information an den Bank-Server.

Der Bank-Server schreibt diese Informationen auf ein Schwarz-Weiß-Bild. Dabei schreibt er – um die Fälschungssicherheit zu garantieren - jede Einzel-Information nicht an eine festgelegte Stelle im Bild, sondern jeweils nur in einen bestimmten festgelegten Bereich des Bildes. Zusätzlich schreibt er in einen bestimmten festgelegten Bereich des Bildes eine zufällig erzeugte Ziffernfolge ("TAN"). Er merkt sich diese TAN. Dann nimmt er eine unverbrauchte Folie und

erzeugt aus dieser und dem erzeugten Bild nach dem Verfahren der Visuellen Kryptographie das zweite Teilgeheimnis-Bild, das er einschließlich dessen Nummer an das Browser-Fenster schickt, an dem der Bankkunde X sitzt. Es ensteht die in **Abb. 5A** dargestellte Situation.

Der Bankkunde X legt die entsprechende Folie auf das Teilgeheimnis-Bild am Bildschirm und sieht die Überweisungsdaten noch einmal bestätigt, siehe Abb. 5B. Wenn die Daten stimmen, tippt er die angezeigte TAN im Klartext in ein dafür vorgesehenes Eingabefeld ein und schickt sie an den Bank-Server.

Der Bank-Server vergleicht die übermittelte Zahl mit der vorher von ihm vergebenen TAN. Wenn beide übereinstimmen, gibt er die Überweisung frei.

Das Verfahren schützt gegen den Man-in-the-Middle Angriff: Zwar ist es für Malware ein Leichtes, die Überweisungsdaten abzulauschen, aber Malware hat keine Chance, die dem Bankkunden angezeigte Bestätigung der Überweisungdaten zu fälschen: Dazu wäre die Kenntnis der Pixel auf der vom Bankkunden aufgelegten Folie nötig. Aus dem gleichen Grund hat Malware kein Chance, die dem Bankkunden angezeigte TAN zu erkennen.

Wenn der Bank-Server also die korrekte TAN empfängt, haben die Informationen über die tatsächlich anstehende Überweisung den Bankkunden X erreicht, und keine vorgespiegelten Informationen. Ein Man-in-the-Middle Angriff ist also mit diesem Verfahren abgewehrt.

Auf ähnliche Weise, wie der Bankkunde mittels Visueller Kryptographie eine Überweisung fälschungssicher bestätigen kann, kann der Bankkunde auch Abbuchungen von seinem Konto fälschungssicher bestätigen, z.B. bei der Abbuchung vom eigenen Konto beim online-Einkauf: wenn der Bank-Server den Abbuchungs-Auftrag vom Verkäufer bekommt, schickt der Bank-Server (z.B. via email, oder via link von der Web-Seite, auf der der Kauf getätigt wurde) eine Bestätigungs-Nachricht an den Konto-Inhaber, siehe **Abb. 6**. Nur wenn dieser

dort mit seiner PIN die Abbuchung bestätigt, wird die Abbuchung durchgeführt. Aus den gleichen Gründen wie bei der Überweisungsbestätigung ist das Verfahren fälschungssicher.

Das dargestellte Verfahren für Online-Bankkonten ist auch gegen das sogenannte Pharming sicher: kein Angreifer kann per Web-Seite erfolgreich vortäuschen, die Bank zu sein, denn das Teilgeheimnis-Bild, was dem Benutzer beim Login zur Eingabe der PIN gezeigt wird, kann nicht gefälscht werden: ohne Kenntnis der Pixel auf der aufzulegenden Folie kann kein Teilgeheimnis-Bild erstellt werden, auf dem zusammen mit der Folie überhaupt etwas zu erkennen ist, denn ein gefälschtes Teilgeheimnis-Bild auf dem Bildschirm und die Folie des Benutzers ergeben übereinandergelegt ein Rauschbild (d.h. ein Bild ohne Information).

Das dargestellte Verfahren macht das sogenannte Phishing für Betrüger uninteressant: Emails oder Web-Seiten, die den Bankkunden betrügerisch nach der PIN fragen, können in dem Fall, dass der Bankkunde die PIN naiverweise preisgibt, mit dieser PIN nichts anfangen: um in den Account hineinzukommen, fehlt ihnen immer noch eine Folie.

Patentansprüche

1) Verfahren zur abhörsicheren Übertragung einer Zeichenreihe von einem Klienten durch ein Rechnernetz zu einem Server, gekennzeichnet durch die folgenden Schritte:

   a) das Erzeugen eines ersten Teilgeheimnis-Bildes gemäß dem Verfahren der Visuellen Kryptographie auf einer Folie durch den Server,

   b) das Erzeugen eines Bildes mit Schaltflächen, die nach dem Zufallsprinzip mit Zeichen beschriftet werden, durch den Server,

   c) das Erzeugen eines zweiten Teilgeheimnis-Bildes gemäß dem Verfahren der Visuellen Kryptographie für das in b) erzeugte Bild durch den Server, welches auf dem Bildschirm des Klienten angezeigt wird, wobei die den Schaltflächen des in b) erzeugten Bildes entsprechenden Flächen des zweiten Teilgeheimnis-Bildes als Schaltflächen durch eine Maus anklickbar sind,

   d) das Übereinanderlegen der Folie und des Bildschirms durch den Klienten, wobei das Bild mit den anklickbaren und mit Zeichen beschrifteten Schaltflächen für den Klienten sichtbar wird,

   e) die Eingabe einer Reihe von n Zeichen durch den Klienten via n Mausklicks auf die beschrifteten Schaltflächen,

   f) die Übertragung der Information darüber, welche Schaltflächen der Klient in welcher Reihenfolge angeklickt hat, zum Server,

   g) die Rekonstruktion der vom Klienten eingegebenen Zeichenreihe durch den Server.

2) Verfahren zur abhör- und fälschungssicheren Übertragung einer Zeichenreihe von einem Server durch ein Rechnernetz zu einem Klienten gekennzeichnet durch die folgenden Schritte:

a) das Erzeugen eines ersten Teilgeheimnis-Bildes gemäß dem Verfahren der Visuellen Kryptographie auf einer Folie durch den Server,

b) das Erzeugen eines Bildes, das mit der zu übertragenden Zeichenreihe beschriftet ist, durch den Server,

c) das Erzeugen eines zweiten Teilgeheimnis-Bildes gemäß dem Verfahren der Visuellen Kryptographie für das in b) erzeugte Bild durch den Server, welches auf dem Bildschirm des Klienten angezeigt wird,

d) das Übereinanderlegen der Folie und des Bildschirms durch den Klienten, wobei das Bild mit der Zeichenreihe für den Klienten sichtbar wird.

3) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass der Bildschirm des Klienten der Bildschirm eines Computers oder eines mobilen Endgerätes ist.

4) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Folie aus Kunststoff oder Papier besteht.

5) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Folie zum Erzeugen des Teilgeheimnis-Bildes mit Farbe bedruckt wird.

6) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Folie zum Erzeugen des Teilgeheimnis-Bildes mit schwarzer oder bunten Farbe bedruckt wird.

7) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Folie zum Erzeugen des Teilgeheimnis-Bildes ausgestanzt wird.

8) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Folie zum Fixieren auf dem Bildschirm mit mindestens einem Klebestreifen versehen ist.

9) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Zeichen auf dem Bild mit Schaltflächen Ziffern, Buchstaben und / oder Sonderzeichen sind.

10) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das Bild mit den anklickbaren und mit Zeichen beschrifteten Schaltflächen einen Nummernfeld darstellt, wobei die Nummer zwischen 0 und 9 jeweils den einzelnen Schaltflächen zugeordnet sind.

11) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Beschriftungen auf den Schaltflächen auf dem Bild einen Verweis auf die Position der anzuklickenden Schaltfläche beinhalten.

12) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Anzahl von Schaltflächen n+m-1 beträgt, wobei m die Anzahl aller für die Eingabe zur Verfügung stehender Zeichen ist.

13) Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Zeichenreihe ein Passwort, ein PIN, ein TAN o.ä. ist.

14) Computerprogrammprodukt zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12, wenn das Computerprogramm auf einem Prozessor ausgeführt wird.

15) Folie zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass sie ein Teilgeheimnis-Bild gemäß dem Verfahren der Visuellen Kryptographie beinhaltet und zum Fixieren auf dem Bildschirm mit mindestens einem Klebestreifen versehen ist.

16) Folie nach Anspruch 14, dadurch gekennzeichnet, dass sie aus einem transparenten Material besteht.

17) Folie nach einem der Ansprüche 14 bis 15, dadurch gekennzeichnet, dass sie mit Farbe bedruckt ist.

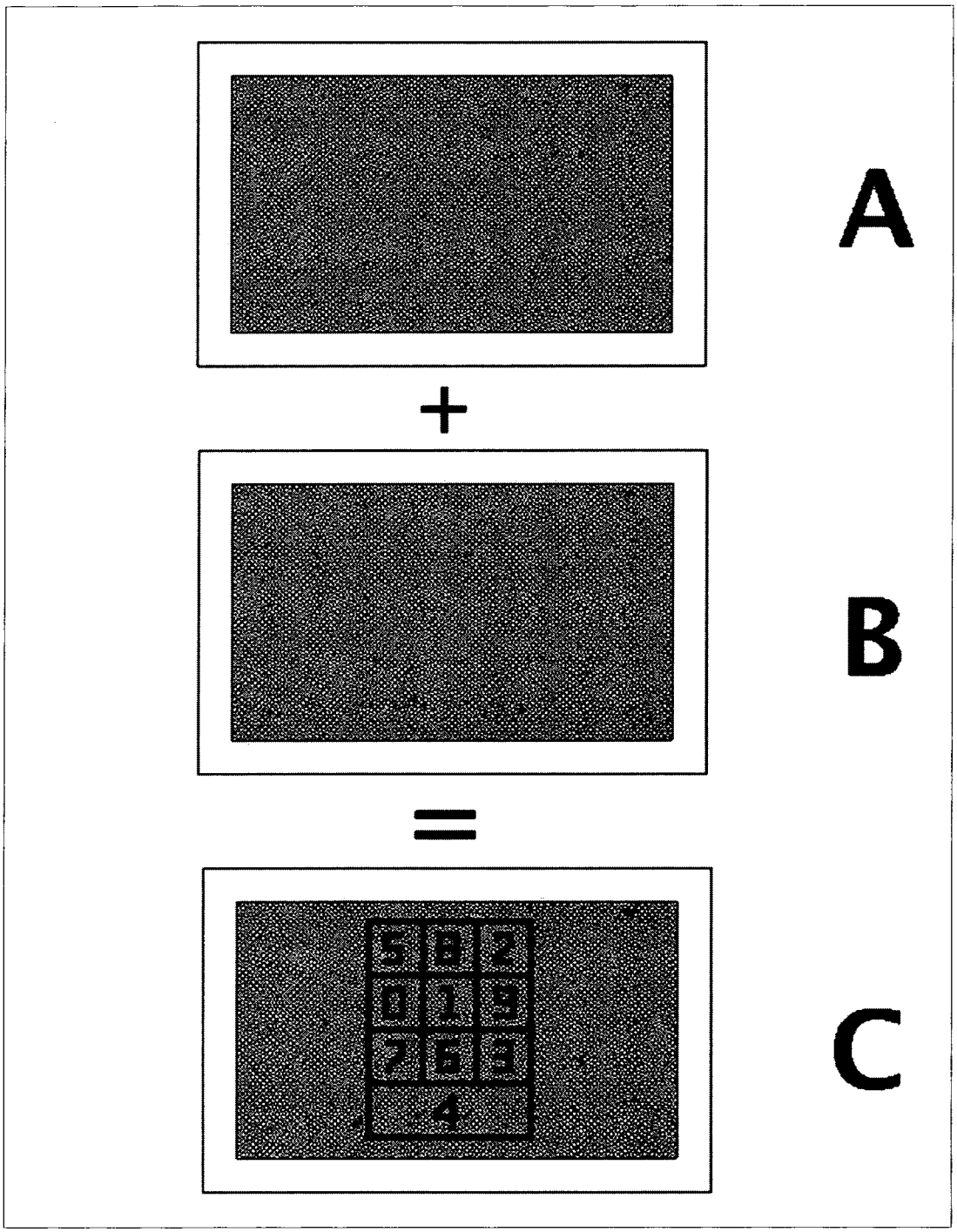
18) Folie nach einem der Ansprüche 14 bis 16, dadurch gekennzeichnet, dass sie mit schwarzer oder bunten Farbe bedruckt ist.

19) Folie nach einem der Ansprüche 14 bis 17, dadurch gekennzeichnet, dass sie ausgestanzt ist.

20) Verwendung des Verfahrens, des Computerprogrammprodukts oder der Folie gemäß einem der vorgehenden Ansprüche bei Online-Accounts.

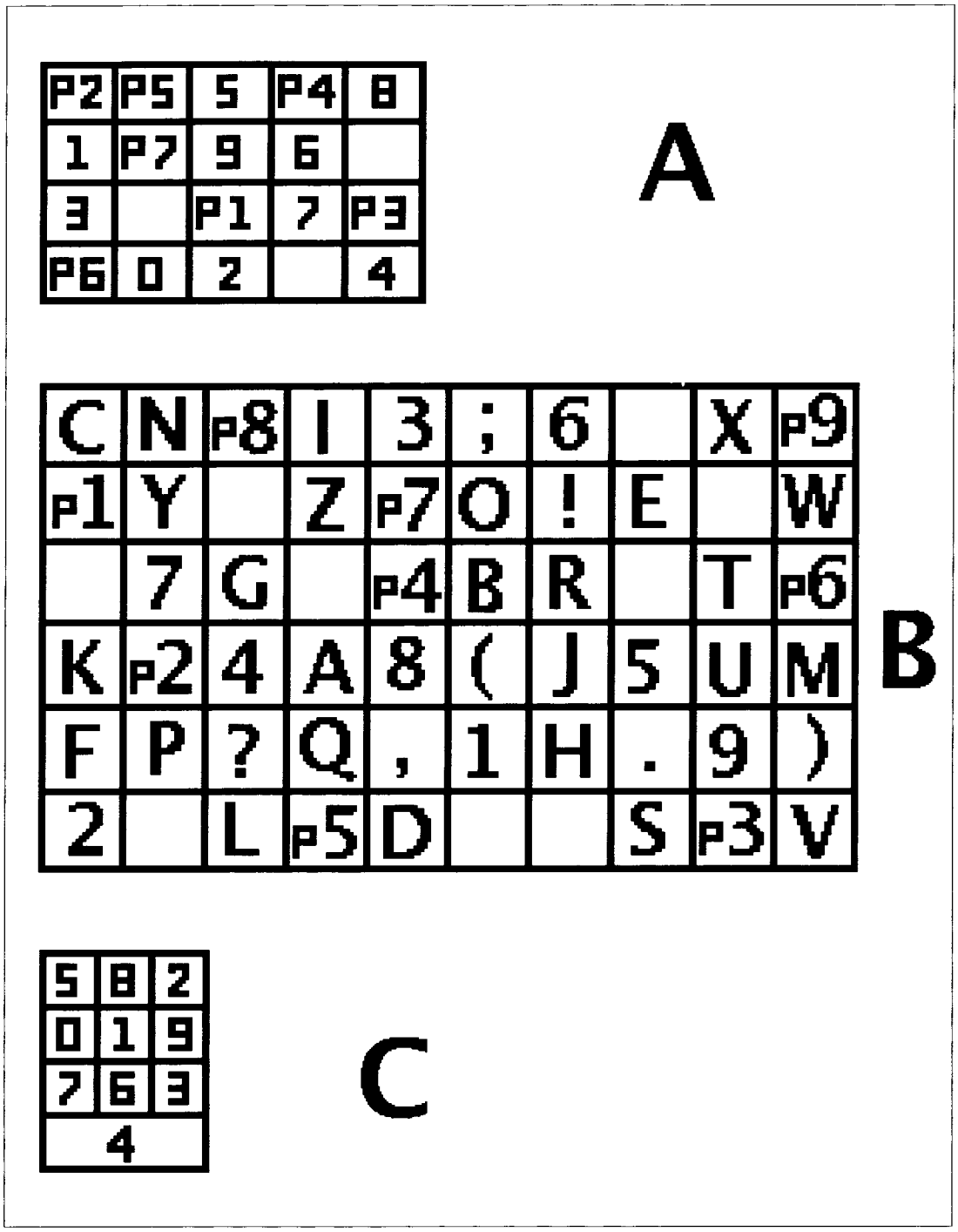
Borchert1

Abb. 1



Borchert1

Abb. 2



Borchert1

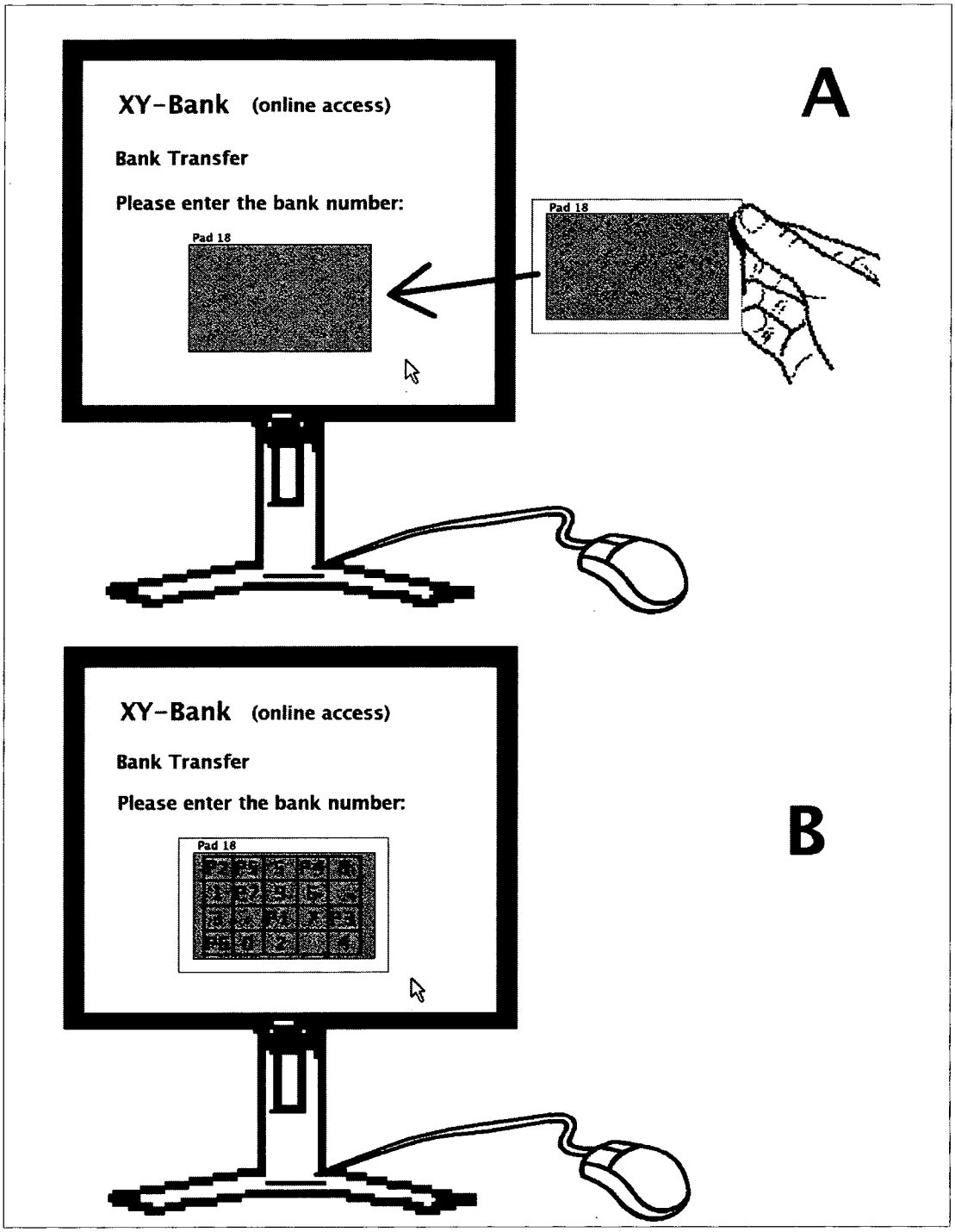
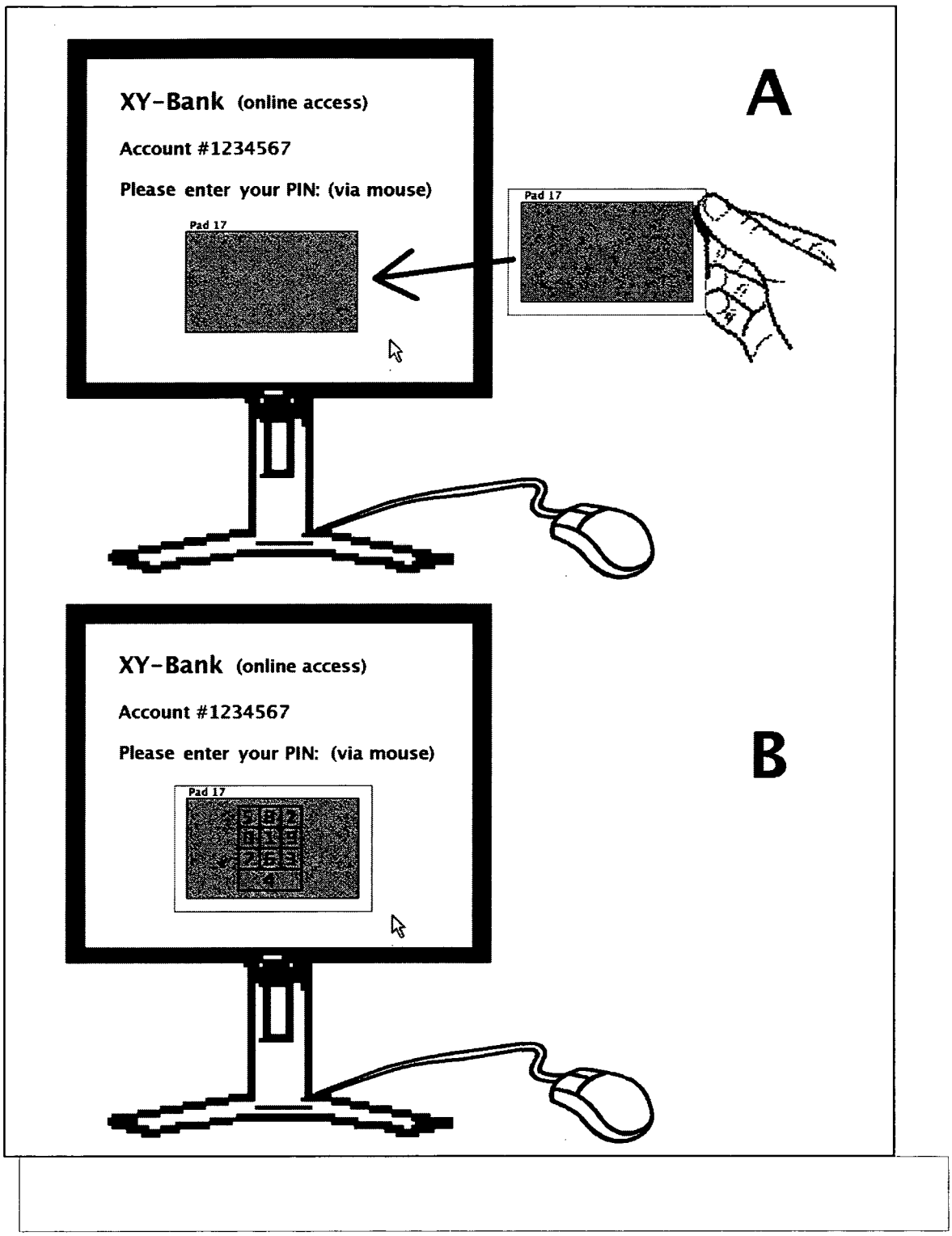


Abb. 3

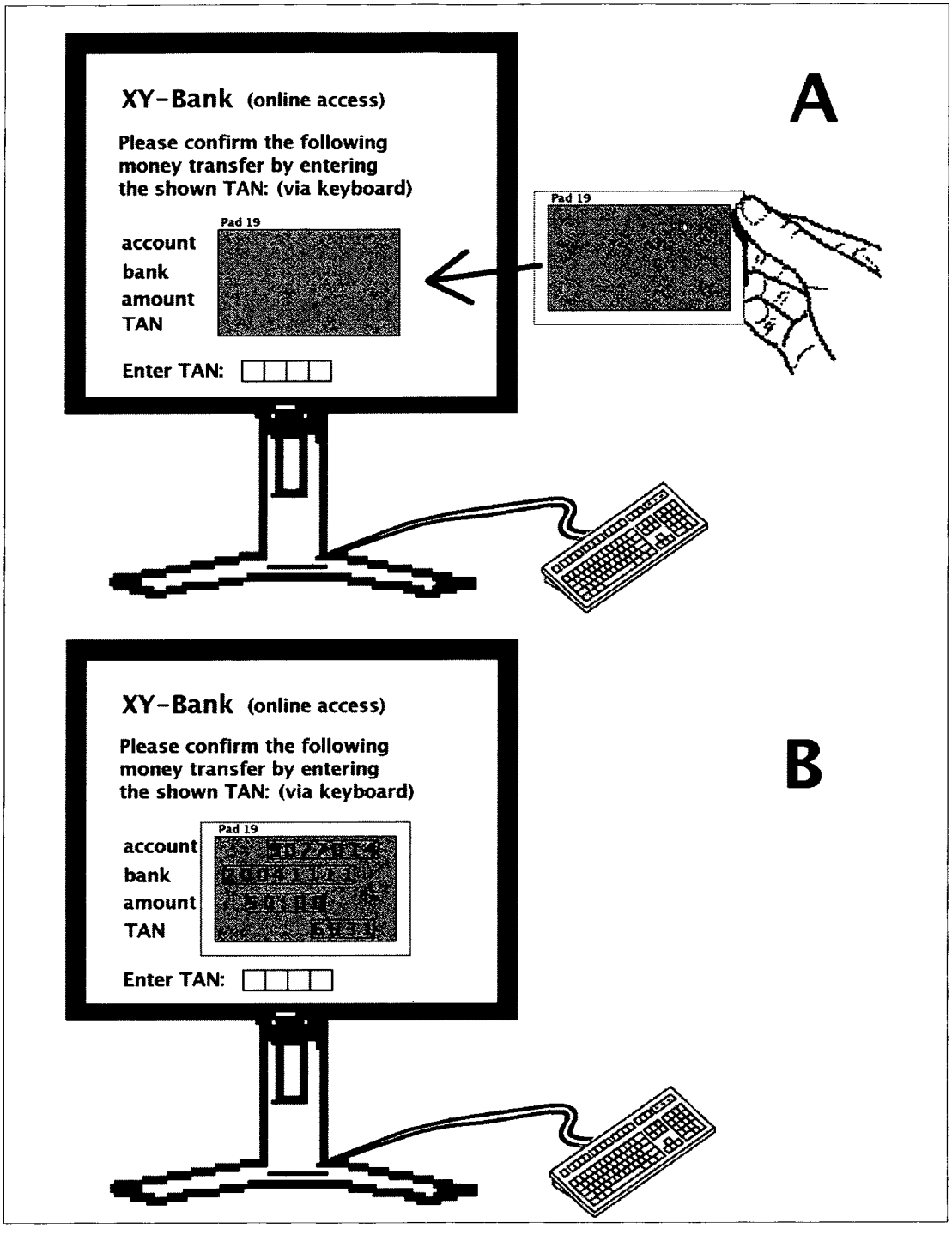
Borchert1

Abb. 4



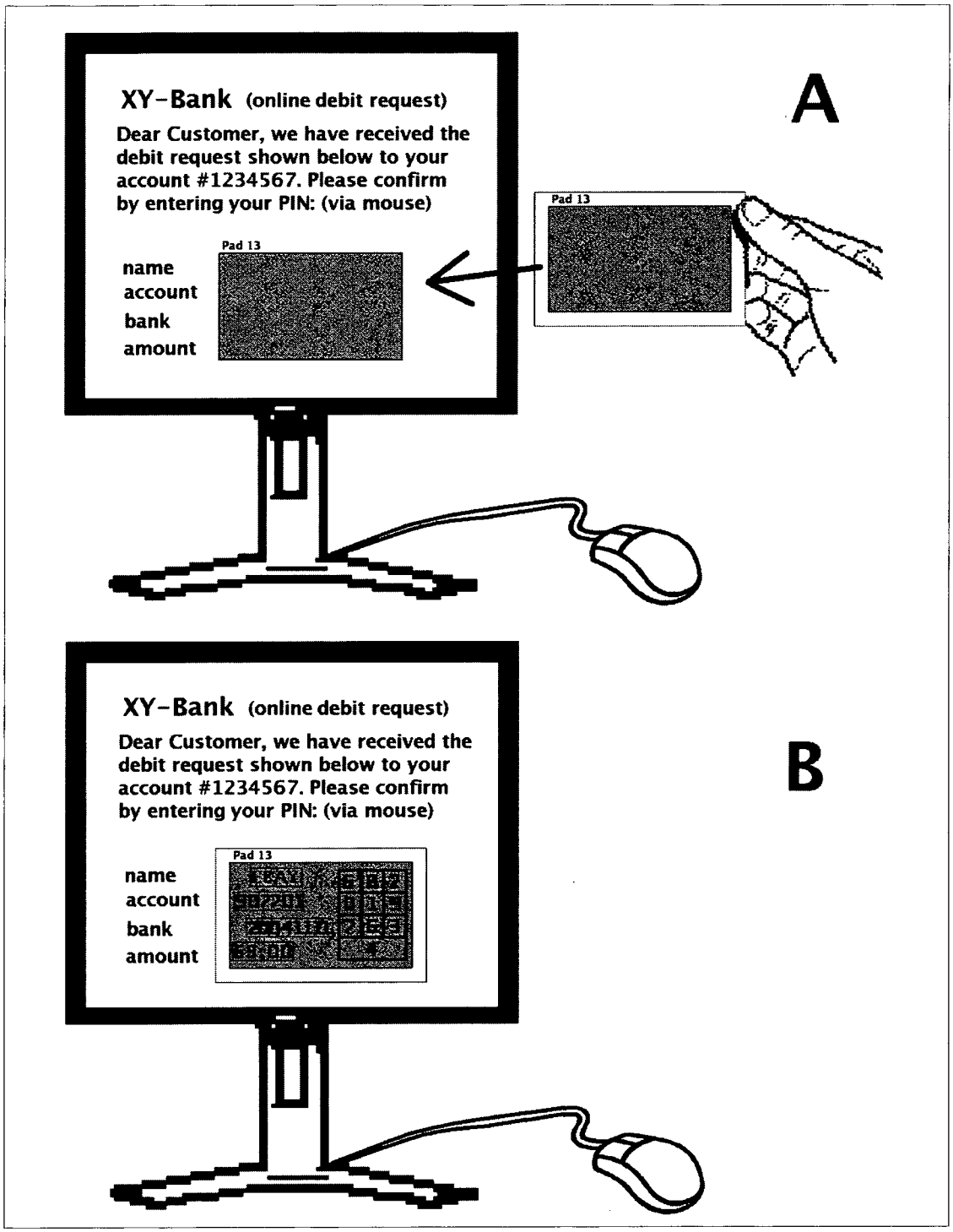
Borchert1

Abb. 5



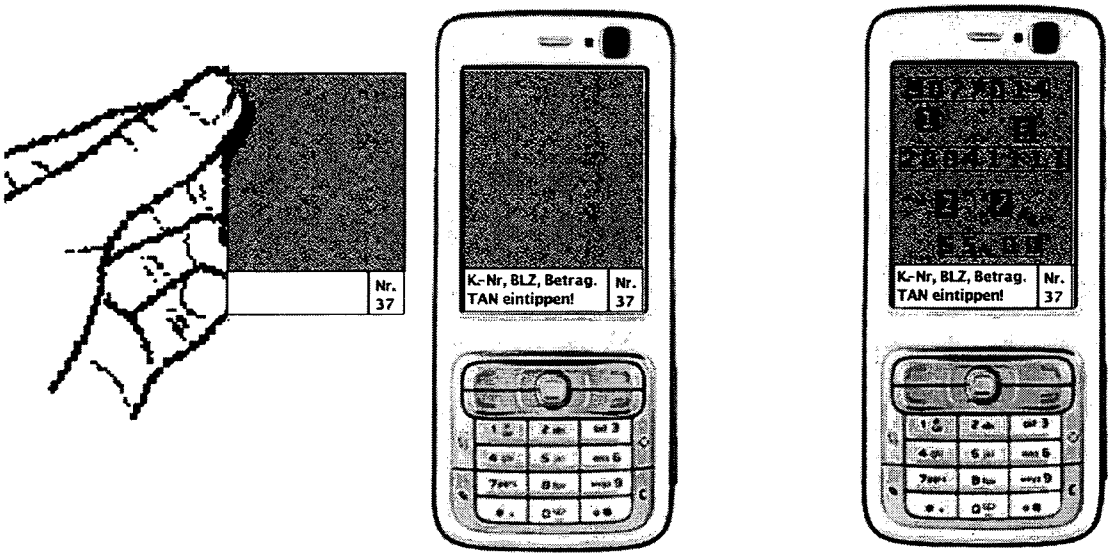
Borchert1

Abb. 6



Borchert1

Abb. 7



Borchert1

Abb. 8