(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 210 573 A1** 2016.12.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 210 573.3**
(22) Anmeldetag: **09.06.2015**
(43) Offenlegungstag: **15.12.2016**

(51) Int Cl.: ***H04L 9/00*** (2006.01)
G06F 21/60 (2013.01)
G06F 3/01 (2006.01)

(71) Anmelder:
Eberhard Karls Universität Tübingen, 72074 Tübingen, DE

(74) Vertreter:
Patentanwaltskanzlei Cartagena Partnerschaftsgesellschaft Klement, Eberle mbB, 70182 Stuttgart, DE

(72) Erfinder:
Burg, Sebastian, 70771 Leinfelden-Echterdingen, DE; Bringmann, Oliver, Prof. Dr., 72074 Tübingen, DE; Peterson, Dustin, 72135 Dettenhausen, DE

(56) Ermittelter Stand der Technik:

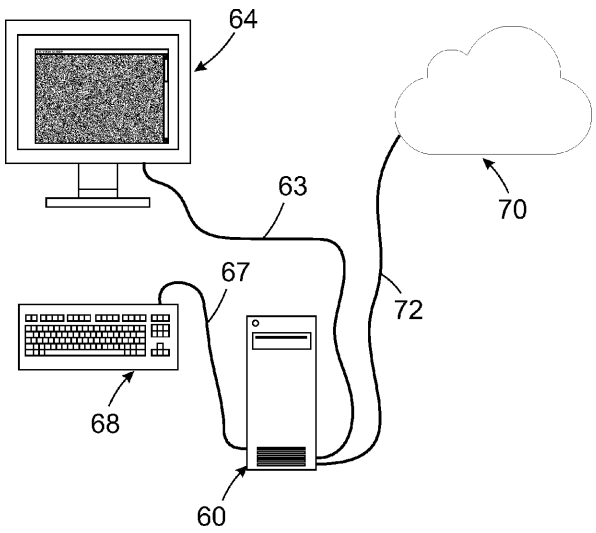
DE	**10 2008 062 872**	**A1**
US	**2011 / 0 264 922**	**A1**
US	**2014 / 0 052 989**	**A1**
EP	**2 684 965**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und System zur Verschlüsselung von Tastendrücken**

(57) Zusammenfassung: Es werden ein Verfahren zur Verschlüsselung von Tastendrücken (20) und ein System zur Durchführung des Verfahrens vorgeschlagen.
Bei dem Verfahren wird ein Videodatenstrom analysiert und aus Bildinformationen (50) des Videodatenstroms eine Schlüsselinformation (53c, 90) zur Verschlüsselung von Tastendrücken (20) ermittelt. Über einen Tastatureingangsanschluss werden erfolgte Tastendrücke (20) an einer angeschlossenen Tastatur (68) erfasst. Die erfassten Tastendrücke (20) werden unter Nutzung einer der Schlüsselinformationen (53c, 90) verschlüsselt, so dass verschlüsselte Tastendrücke (22) erzeugt werden. Über einen Tastaturausgangsanschluss werden die verschlüsselten Tastendrücke (22) an eine Zentraleinheit weitergegeben.
Verwendung zur Übertragung von Nutzereingaben an eine Gegenstelle, ohne dass durch ein von Schadsoftware befallenen Computer des Nutzers die Eingaben



Beschreibung

ANWENDUNGSGEBIET UND STAND DER TECHNIK

[0001] Die Erfindung betrifft ein Verfahren zur Verschlüsselung von Tastendrücken nach dem Oberbegriff von Anspruch 1 sowie ein System zur Verschlüsselung von Tastendrücken nach dem Oberbegriff von Anspruch 5.

[0002] Aus dem Stand der Technik sind Systeme bekannt, die die Übertragung von Bildinformationen von einem Quellrechner (Gegenstelle) zu einem Zielrechner in verschlüsselter Form gestatten. Eine solche Technik ist aus der DE 102008062872 A1 bekannt.

[0003] Die Besonderheit dieses Verfahrens liegt darin, dass die Bildinformationen mangels Schlüsselinformationen auch vom Zielrechner noch nicht entschlüsselt werden können. Erst eine Dekodier-Einheit, die zwischen dem Videoausgang der Zentraleinheit des Zielrechners und dessen Bildschirm angeordnet ist, kann die Entschlüsselung vornehmen. Die Besonderheit dieses bekannten Verfahrens liegt dementsprechend darin, dass selbst ein kompromittierter Zielrechner, auf dem beispielsweise eine Trojaner-Software läuft, keine Gefahr darstellt, denn er ist bestimmungsgemäß nicht selbst in der Lage zu einer Entschlüsselung der Bilddaten. Aufgabe des Zielrechners ist es lediglich, verschlüsselt erhaltene Bildinformationen in weiterhin verschlüsselter Form am Grafikausgang des Rechners auszugeben. Das Verfahren ist in **Fig.** 1b verdeutlicht. Bilddaten von einer Gegenstelle **70** werden von der Zentraleinheit **60** des Zielrechners ohne vorherige Entschlüsselung weitergeleitet in Richtung des Bildschirms **64**. Erst durch die Dekodier-Einheit **62** erfolgt die Entschlüsselung, so dass die Bilddaten entschlüsselt am Bildschirm **64** dargestellt werden können.

[0004] Dieses Verfahren hat sich als hochsicheres Verfahren bewährt.

[0005] Allerdings ist mit diesem Verfahren ein sicherer Rückkanal zur Gegenstelle nur eingeschränkt möglich. Zwar kann die Trojaner-Software bei einem Verfahren beschriebener Art die Bildinformationen nicht entschlüsseln. Die Tastatureingaben eines Benutzers jedoch können von der Trojaner-Software mitgelesen werden.

[0006] Um dieses Problem zu umgehen, ist in genannter Schrift vorgeschlagen worden, Eingaben nicht über die reale Tastatur des Zielrechners erfolgen zu lassen, sondern über eine als Bildinformation übermittelte und auf dem Bildschirm dargestellte Tastatur, die per Maus bedient wird. Eine möglicherweise vorhandene Trojaner-Software kann dann zwar die Koordinaten eines Mausklicks auf der auf dem Bildschirm dargestellten Tastatur erfassen. Er kennt jedoch die Bedeutung dessen nicht.

[0007] Obwohl sich sowohl das beschriebene Verfahren zur verschlüsselten Übermittlung von Bildinformationen als auch die Eingabe über eine ebenfalls am Bildschirm dargestellte und mit der Maus zu bedienende Tastatur bewährt haben, verbleibt doch der Nachteil, dass längere Texteingaben auf diesem Wege äußerst unbequem sind.

AUFGABE UND LÖSUNG

[0008] Aufgabe der Erfindung ist es, ein Verfahren zur sicheren Übermittlung von Tastatureingaben von einem ersten Rechner zu einem zweiten Rechner zur Verfügung zu stellen, dessen Sicherheit nicht davon abhängt, dass der erste Rechner frei von Schadsoftware ist.

[0009] Die der Erfindung zugrunde liegende Aufgabe wird ein Verfahren zur Verschlüsselung von Tastendrücken nach Anspruch 1 gelöst.

[0010] Gemäß diesem Verfahren, welches vorzugsweise auf einer als Zwischeninstanz agierenden Einheit zwischen der Zentraleinheit und dem Bildschirm und der Tastatur durchgeführt wird, wird ein Videodatenstrom analysiert und aus Bildinformationen des Videodatenstroms wird eine Schlüsselinformationen zur Verschlüsselung von Tastendrücken ermittelt. Über einen Tastatureingangsanschluss werden erfolgte Tastendruckinformationen einer angeschlossenen Tastatur erfasst. Die erfassten Tastendrücke werden unter Nutzung einer der aus dem Videodatenstrom extrahierten Schlüsselinformationen verschlüsselt, so dass verschlüsselte Tastendrücke erzeugt werden. Über einen Tastaturausgangsanschluss werden dann die verschlüsselten Signale zu den Tastendrücke an eine Zentraleinheit weitergegeben.

[0011] Bei dem Verfahren ist es demnach vorgesehen, dass die Auswertung von Tastendrücken an einer realen Tastatur zunächst nicht von der Zentraleinheit selbst, sondern von einer separaten Zwischeninstanz vorgenommen wird, an der die Tastatur angeschlossen ist. Diese wiederum ist mit der Zentraleinheit verbunden, wobei sich die Zwischeninstanz vorzugsweise selbst als Tastatur ausgibt. Im Falle einer USB-Verbindung würde sie demnach vorzugsweise als USB-Gerät mit HID-Profil (Human Interface Device) agieren.

[0012] Die das Verfahren ausführende Zwischeninstanz verschlüsselt bestimmungsgemäß die von der Tastatur stammenden Signale hinsichtlich betätigter Tasten, wobei diese Verschlüsselung vorzugsweise dergestalt ist, dass ein Tastendruck an der realen

Tastatur als Tastendruck, jedoch einer anderen Taste, an die Zentraleinheit weitergegeben wird.

[0013] Grundsätzlich wäre es denkbar, dass die Zwischeninstanz über eine statische Schlüsselinformation verfügt, mittels derer die Verschlüsselung erfolgt. Dies würde jedoch damit einhergehen, dass die Verschlüsselung immer auf gleiche Weise vonstattengeht, also der gleiche Tastendruck an der realen Tastatur zum gleichen an die Zentraleinheit weitergegebenen Tastendruck führt. Eine solche Form der Verschlüsselung wäre anfällig für einfache Häufigkeitsanalysen.

[0014] Beim erfindungsgemäßen Verfahren ist demnach vorgesehen, dass die Schlüsselinformation zur Verschlüsselung des Tastendrucks sich für jeden Tastendruck oder gruppenweise für mehrere infolge stattfindende Tastendrücke verändert. Die erforderliche veränderliche Schlüsselinformation wird einem Videodatenstrom entnommen, der vom Videoausgang der Zentraleinheit an den Bildschirm weitergegeben wird.

[0015] Diese Schlüsselinformation kann insbesondere in Form von Farbwerten von Pixeln eines Bildes des Videodatenstroms übertragen werden. Diese Pixel, die die Schlüsselinformation beinhalten, sind vorzugsweise Teil eines Bereichs des Einzelbildes des Videodatenstroms, in welchem verschlüsselte Bilddaten und zur Entschlüsselung erforderliche Kopfdaten hierfür abgelegt sind, die bestimmungsgemäß durch eine Dekodier-Einheit entschlüsselt werden, wenn der Videodatenstrom der Dekodier-Einheit zugeführt wird.

[0016] Für die Verteilung von Schlüsselinformationen zur Verschlüsselung von Tastendrücken in den Einzelbildern eines Videodatenstroms bestehen verschiedene Möglichkeiten. So kann ein Einzelbild beispielsweise eine Vielzahl unterschiedlicher Schlüsselinformationen enthalten, die anschließend für Tastendrücke nacheinander Verwendung finden. Auch ist es möglich, dass jedes Einzelbild nur maximal eine Schlüsselinformation enthält, welche dann nur für den jeweils nächsten Tastendruck Verwendung findet.

[0017] Das genannte Verfahren wird in der beschriebenen Weise auf einer Rechneranlage durchgeführt, der mit einer Gegenstelle kommuniziert. Diese Gegenstelle ist Quelle der Bildinformationen, die mittelbar als Teil des Videodatenstroms über den Videoausgang des Zielrechners ausgegeben werden und die Verschlüsselungsinformationen tragen. Die Gegenstelle ist auch Empfänger der verschlüsselten Tastendrücke. Da sie zuvor die Verschlüsselungsinformation in Form von Bilddaten festgelegt hat, ist sie in der Lage, die verschlüsselten Tastendrücke wieder zu entschlüsseln, um zum vom Benutzer eingegebenen Klartext zu gelangen.

[0018] Die Schlüsselinformation zur Verschlüsselung von Tastendrücken kann im Videodatenstrom vorzugsweise in wiederum verschlüsselter Form vorliegen. Hierdurch wird verhindert, dass eine Instanz zwischen dem Zielrechner und der Gegenstelle oder die Zentraleinheit des Zielrechners selbst in der Lage ist, die Schlüsselinformation auszulesen und infolgedessen darauf folgende Tastendrücke entschlüsseln zu können. Vorzugsweise ist die Schlüsselinformation mit dem öffentlichen Schlüssel eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt in Farbwerten von Pixeln des übertragenen Bildes kodiert, wobei der korrespondierende private Schlüssel nur auf der das Verfahren durchführenden Dekodier-Einheit oder auf einer für die Dekodier-Einheit zugänglichen Smartcard abgelegt ist.

[0019] Bei der Verschlüsselung der erfassten Tastendrücke kann eine Verschiebungs-Verschlüsselung unter Nutzung eines Verschiebungswertes Anwendung finden. Dieser Verschiebungswert kann Teil der im Videodatenstrom enthaltenen Schlüsselinformationen sein.

[0020] Die Verschlüsselung in Art einer Verschiebungsverschlüsselung bedeutet, dass alle denkbaren Tastendrücke oder ein Teil hiervon eine Liste definierter Reihenfolge darstellen, in der in Abhängigkeit eines Verschiebewertes n der tatsächlich erfolgte Tastendruck in einen verschlüsselten Tastendruck umgewandelt wird, der in genannter Reihenfolge n Elemente nach oder vor dem erfolgten Tastendruck vorgesehen ist. Ein solches Verfahren wird auch Cäsarenverschlüsselung genannt.

[0021] Vereinfacht ausgedrückt könnte man in Hinblick auf die Buchstaben des Alphabetes eine Verschiebeverschlüsselung dadurch erzielen, dass ausgehend von einem erfolgten Tastendruck eine Anzahl von Zeichen nach vorne oder zurückgezählt wird, um den verschlüsselten Tastendruck zu erzeugen. Die genannte Anzahl von Zeichen stellt die Schlüsselinformation dar. Beispielsweise würde in diesem einfachen Beispiel eine Schlüsselinformation +3 dazu führen, dass der unverschlüsselte Buchstabe A zum verschlüsselten Buchstaben D würde, der unverschlüsselte Buchstabe B zum verschlüsselten Buchstaben E, usw.

[0022] Diese besonders einfache Art der Verschlüsselung bietet sich insbesondere deshalb an, da es mit ihr besonders einfach ist, erfolgte Tastendrücke so zu verschlüsseln, dass das Ergebnis wiederum einen Tastendruck darstellt. Hierdurch kann die Weiterverarbeitung des verschlüsselten Tastendrucks am Zielrechner in besonders einfacher Weise erfolgen.

[0023] Die Schlüsselinformationen zur Verschlüsselung von Tastendrücken, die aus dem Videodatenstrom ermittelt wird, kann eine Mehrzahl von nacheinander zu verwendenden Einzelschlüsselinformationen umfassen, die gemeinsam in einem gemeinsamen Einzelbild des Videodatenstroms enthalten sind.

[0024] Durch die Übersendung einer Mehrzahl von Schlüsselinformationen zur sequentiellen Abarbeitung bei der Verschlüsselung in einem Einzelbild wird ein vergleichsweise störunanfälliges Verfahren ermöglicht. Durch die Übersendung der Schlüsselinformationen in Form von Bilddaten kann die Dekodier-Einheit einen Stack mit Schlüsselinformationen füllen, von dem nach dem FIFO-Prinzip (First-In/First-Out) Schlüsselinformationen zur Verschlüsselung erfolgender Tastendrücke entnommen werden. Sinkt die Anzahl der im Stack noch zur Verfügung stehenden Schlüsselinformationen, kann die Gegenstelle im Rahmen eines Einzelbildes eine Vielzahl neuer Schlüsselinformationen senden, die dann für weitere Tastendrücke und deren Verschlüsselung Verwendung finden.

[0025] Die der Erfindung zugrunde liegende Aufgabe wird auch ein System zur Verschlüsselung von Tastendrücken nach Anspruch 5 gelöst.

[0026] Dieses System verfügt über eine Video-Dekodier-Einheit mit einem Videoeingangsanschluss sowie über eine Tastatur-Enkodier-Einheit mit einem Tastatureingangsanschluss zum Anschließen einer Tastatur und einem Tastaturausgangsanschluss zum Anschließen an eine Zentraleinheit.

[0027] Das System ist zur Durchführung des beschriebenen Verfahrens ausgebildet.

[0028] Die Video-Dekodier-Einheit und die Tastatur-Enkodier-Einheit können in Form eines Gerätes oder mehrerer Geräte vorliegen. Nach außen hin verfügt ein solches System zumindest über einen Videoeingangsanschluss, über den die Bildinformationen mit den Schlüsselinformationen empfangen werden können. Es verfügt weiterhin über einen Tastatureingangsanschluss, der Signale von Tastendrücken von einer angeschlossenen Tastatur entgegennimmt, und einen Tastaturausgangsanschluss, über die die Signale zu verschlüsselten Tastendrücken an die Zentraleinheit des Zielrechners weitergegeben werden können.

[0029] Bei dem Videoeingangsanschluss handelt es sich vorzugsweise um einen digitalen Videoeingangsanschluss wie DVI-D, HDMI oder Display Port. Ein digitales Bildsignal ist für die Extraktion von Schlüsselinformationen erheblich besser geeignet als ein analoges, bei dem zunächst eine D/A-Wandlung erforderlich ist. Der Tastatureingangsanschluss und der Tastaturausgangsanschluss können jeweils insbesondere als USB oder PS/2-Anschluss vorliegen.

[0030] Das System verfügt vorzugsweise auch über einen Videoausgangsanschluss, über den der Videodatenstrom in ursprünglicher oder manipulierter Form an einen Bildschirm weitergegeben wird. In einem solchen Fall ist das System somit einerseits zwischen Zentraleinheit und Bildschirm und andererseits zwischen Zentraleinheit und Tastatur eingefügt.

[0031] Das System lässt bestimmungsgemäß keinen Zugriff von Seiten der Zentraleinheit zu, durch die die unverschlüsselten Tastendruckinformationen oder anderweitige zur Entschlüsselung geeignete Informationen der Zentraleinheit preisgegeben würden.

[0032] Die Video-Dekodier-Einheit und die Tastatur-Enkodier-Einheit können Teil eines gemeinsamen Gerätes sein.

[0033] Die Integration der Video-Dekodier-Einheit und der Tastatur-Enkodier-Einheit in einem gemeinsamen Gerät schafft eine besonders bedienerfreundliche Gestaltung. Das Gerät muss lediglich mit der Zentraleinheit und der Tastatur sowie dem Videoausgang der Zentraleinheit verbunden werden. Je nach Ausgestaltung muss weiterhin ein Bildschirm am Videoausgang dieses gemeinsamen Gerätes angeschlossen werden.

[0034] Die Video-Dekodier-Einheit und die Tastatur-Enkodier-Einheit können auch als getrennte Einheiten ausgebildet sein, die über eine Kabelverbindung miteinander verbunden sind.

[0035] Die Ausgestaltung der Video-Dekodier-Einheit und der Tastatur-Enkodier-Einheit als getrennte Einheiten, die miteinander über eine Datenleitung verbunden sind, gestattet es, die Tastatur-Enkodier-Einheit nur dann in das Gesamtsystem zu integrieren, wenn diese benötigt wird. Da die Video-Dekodier-Einheit auch ohne Tastatur-Enkodier-Einheit eine sinnvolle Verwendung zulässt, kann somit ein vorteilhaftes modulares System geschaffen werden.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0036] Weitere Vorteile und Aspekte der Erfindung ergeben sich aus den Ansprüchen und aus der nachfolgenden Beschreibung von bevorzugten Ausführungsbeispielen der Erfindung, die nachfolgend anhand der stark schematisierten Figuren erläutert sind.

[0037] Fig. 1A zeigt ein Computersystem, welches mit einer Gegenstelle verbunden ist und welches einen Bildschirm zur Darstellung von von der Gegenstelle stammenden Informationen sowie eine Tastatur zur Eingabe von Zeichen zur Übersendung an die Gegenstelle aufweist.

[0038] **Fig.** 1B zeigt ein Computersystem, das zusätzlich zu den Komponenten des Computersystems gemäß **Fig.** 1A ein Gerät zwischen der Zentraleinheit und dem Bildschirm aufweist, welches als Dekodier-Einheit für den Videodatenstrom agiert.

[0039] **Fig.** 2 zeigt ein Computersystem, welches in Übereinstimmung mit der Gestaltung der **Fig.** 1B ein eine Dekodier-Einheit beinhaltendes Gerät zwischen Zentraleinheit und Bildschirm aufweist, wobei dieses Gerät zusätzlich eine Enkodier-Einheit zur Verschlüsselung von Tastaturdrucksignalen aufweist.

[0040] **Fig.** 3A bis **Fig.** 3D verdeutlichen die Dekodierung des Videodatenstroms einschließlich der Entgegennahme von Schlüsselinformationen zur späteren Verschlüsselung von Tastendrücken.

[0041] **Fig.** 4 zeigt die Verfahrensschritte zur Tastaturverschlüsselung von der Identifikation und Extraktion von Schlüsselinformationen aus dem Videodatenstrom bis zur Anwendung dieser Schlüsselinformationen zur Verschlüsselung von Tastendrücken.

[0042] **Fig.** 5A und **Fig.** 5B verdeutlicht die Verschlüsselung von Tastendrücken anhand eine Verschiebe-Verschlüsselung mit veränderlichem Verschiebewert (Schlüsselinformation).

DETAILLIERTE BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

[0043] Die **Fig.** 1A und **Fig.** 1B dienen der Erläuterung, zeigen selbst jedoch keine erfindungsgemäßen Systeme.

[0044] **Fig.** 1A zeigt ein Computersystem bestehend aus einer Zentraleinheit **60**, einem Bildschirm **64** sowie einer Tastatur **68**. Das Computersystem ist mit einer Gegenstelle **70** verbunden. Diese Gegenstelle **70** kann ein Server im Internet oder einem internen Netzwerk sein.

[0045] Das Computersystem ist dafür vorgesehen, Informationen von der Gegenstelle **70** auf dem Bildschirm **64** darzustellen. Weiterhin ist es dafür vorgesehen, Tastendrücke des Benutzers auf der Tastatur **68** an die Gegenstelle **70** weiterzugeben.

[0046] Bei einem konventionellen System, wie es in **Fig.** 1A dargestellt ist, werden die darzustellenden Informationen der Gegenstelle **70** zwar möglicherweise auf dem Datenpfad **72** bis zur Zentraleinheit **60** verschlüsselt, müssen dort jedoch durch diese entschlüsselt werden, um auf dem Bildschirm dargestellt zu werden. Dies führt dazu, dass eine Trojaner-Software, die die Zentraleinheit **60** kompromittiert haben könnte, in der Lage ist, entschlüsselte Informationen zu erlangen und an Unbefugte weiterzugeben. Sie kann dies erreichen, indem sie tatsächlich die zur Entschlüsselung verwendeten Schlüssel von der Zentraleinheit **60** entwendet oder die zur Ausgabe vorgesehenen entschlüsselten Bilddaten abgreift.

[0047] **Fig.** 1B verdeutlicht eine bereits bekannte Lösung, um dies zu verhindern. Die Bilddaten, die von der Gegenstelle **70** an die Zentraleinheit **60** des Systems übertragen werden, sind hierbei verschlüsselt, und zwar in einer Art, dass auch die verschlüsselten Bilddaten als Bilddaten interpretiert werden können und somit in ihrer verschlüsselten Form in Richtung des Bildschirmes **64** gesendet werden können, ohne dass die Zentraleinheit zur Entschlüsselung befähigt sein muss. Im Falle des Computersystems der **Fig.** 1A führt dies zur Darstellung dieser verschlüsselten Daten, die dann naturgemäß durch einen Benutzer nicht zu lesen sind. Das System gemäß **Fig.** 1B sieht daher zwischen der Zentraleinheit **60** und dem Bildschirm **64** eine Dekodier-Einheit **62** vor, die über eine zur Entschlüsselung erforderliche Schlüsselinformation, insbesondere den privaten Schlüssel eines asymmetrischen Verschlüsselungsverfahrens, verfügt, welcher auf einer Smartcard **66** abgelegt ist. Hierdurch kann die Dekodier-Einheit **62** bei Erkennen verschlüsselter Bilddaten deren Entschlüsselung vornehmen, so dass eine entschlüsselte Darstellung auf dem Bildschirm stattfindet, ohne dass hierdurch eine Trojaner-Software auf der Zentraleinheit **60** die Möglichkeit erlangen würde, die entschlüsselten Bilddaten abzugreifen.

[0048] Um es darüber hinaus zu gestatten, dass der Benutzer Tastatureingaben machen kann, die über die Zentraleinheit **60** an die Gegenstelle **70** gesendet werden, ohne dass eine Trojaner-Software diese unverschlüsselt abgreifen kann, ist das System gemäß **Fig.** 2 vorgesehen.

[0049] Statt der Dekodier-Einheit **62** der Ausgestaltung der **Fig.** 1B ist hier eine integrierte Dekodier- und Enkodier-Einheit **62** vorgesehen. Diese ist in gleicher Weise wie die Dekodier-Einheit **62** gemäß **Fig.** 1B mit einem Videoausgang der Zentraleinheit verbunden, um in der Lage zu sein, den Videodatenstrom abzugreifen, der von der Zentraleinheit **60** an den Bildschirm **64** gesendet wird. Die Dekodier- und Enkodier-Einheit der **Fig.** 2 ist darüber hinaus jedoch mit einer ersten Datenleitung **67a** mit der Tastatur **68** verbunden und mit einer zweiten Datenleitung **67b** mit einem Tastaturanschluss an der Zentraleinheit **60** verbunden.

[0050] Somit passiert nicht nur der Videodatenstrom die Dekodier- und Enkodier-Einheit **62**, sondern auch der von der Tastatur **68** stammende Datenstrom, bestehend aus Signalen zu einzelnen durch den Benutzer erfolgten Tastendrücken.

[0051] Über die Datenleitung **67b** verhält sich die Dekodier- und Enkodier-Einheit **62** gegenüber der

Zentraleinheit **60** wie eine Tastatur, beispielsweise durch Simulieren eines entsprechenden USB-Protokolls (HID – Human Interface Device). Die Tastatur **68** selbst kann ebenfalls eine übliche USB-Tastatur sein und mittels eines USB-Anschlusses an der Dekodier- und Enkodier-Einheit **62** angeschlossen sein. Die Videoübertragung von der Zentraleinheit bis zur Dekodier- und Enkodier-Einheit **62** und weiter zum Bildschirm **64** erfolgt vorzugsweise über HDMI, DVI-D oder Display Port.

[0052] Anhand der **Fig.** 3A bis **Fig.** 3D wird verdeutlicht, wie die Dekodier- und Enkodier-Einheit **62** den über die Datenleitung **63a** empfangenen Videodatenstrom verarbeitet.

[0053] **Fig.** 3A zeigt ein Einzelbild **50** dieses Videodatenstroms, wie es bei der Dekodier- und Enkodier-Einheit **62** ankommt. Innerhalb eines außen liegenden unverschlüsselten Bereichs ist der Inhalt **52** eines Fensters verschlüsselt. **Fig.** 3B und **Fig.** 3C zeigen, dass neben den eigentlichen Bildinformationen **54** in verschlüsselter Form auch ein Kopfbereich **53** in Form einer Pixelreihe mit Pixeln verschiedener Farbwerte vorgesehen ist, durch den die Dekodier- und Enkodier-Einheit **62** das Vorhandensein verschlüsselter Bildinformationen erkennen kann und weitere Informationen hierzu erhält, beispielsweise Schlüsselinformationen zur Entschlüsselung des Bildes **53b** und eine Marker-Signatur **53a**, um zu erkennen, wo diese Bildinformationen **54** im Einzelbild **50** angeordnet sind. Gemäß dem hier beschriebenen Verfahren zur Tastaturverschlüsselung umfassen die von der Dekodier- und Enkodier-Einheit analysierten Daten auch Schlüsselinformationen **53c** für eine nachfolgende Verschlüsselung von Tastendrücken. Aus der Kopfzeile **53** gemäß **Fig.** 3B können beispielsweise die im Stack **30** der Fig. dargestellten Schlüsselinformationen entnommen werden, wobei es sich im vorliegenden einfachen Beispiel um schlichte Zahlenwerte handelt.

[0054] Die Schlüsselinformationen **53c** ist in **Fig.** 3C zur Vereinfachung unverschlüsselt dargestellt. In der Praxis ist es von Vorteil, wenn diese mit dem öffentlichen Schlüssel eines Schlüsselpaares verschlüsselt sind, dessen privater Schlüssel auf der Smartcard **66** abgelegt ist.

[0055] Die Kopfinformationen gestatten es der Dekodier- und Enkodier-Einheit **62**, die verschlüsselten Bilddaten zu entschlüsseln, so dass das Einzelbild als Teil eines manipulierten Videodatenstroms über die Leitung **63b** in der in **Fig.** 3C dargestellten Form übermittelt wird. Der Bildschirm **64** ist somit zur unverschlüsselten Darstellung der Bilddaten in der Lage.

[0056] Anhand der **Fig.** 4 werden die Schritte zur Verschlüsselung der Tastatursignale verdeutlicht.

[0057] Mit Eingang der Einzelbilder in die Dekodier- und Enkodier-Einheit **62** wird in einem ersten Verfahrensschritt **81** eine Prüfung vorgenommen, ob das Einzelbild Informationen zur Tastaturverschlüsselung enthält. Hierfür wird üblicherweise zunächst nach der definierten Marker-Signatur **53a** aus mehreren Pixeln definierter Farbwerte gesucht, die zu erkennen geben, dass Informationen für die Dekodier- und Enkodier-Einheit **62** im Videodatenstrom enthalten sind.

[0058] Ist dies der Fall und liegen insbesondere auf die Marker-Signatur **42a** folgend Tastaturschlüsselinformationen **53c** in den Bilddaten vor, so werden diese im Schritt **82** extrahiert, gegebenenfalls entschlüsselt und in einem Speicher der Dekodier- und Enkodier-Einheit **62** abgelegt.

[0059] Dieser Speicher ist in **Fig.** 5a als Stack **90** dargestellt. Neu ermittelte Schlüsselinformationen werden von oben auf diesen Stack hinzugefügt. Exemplarisch werden hier in dieser Reihenfolge die Werte **2**, **21**, **14**, **7**, **11**, **1**, **22**, **3** eingefügt.

[0060] Erfolgt ein Tastendruck an der Tastatur **68**, so wird dies durch die Dekodier- und Enkodier-Einheit **62** im Schritt **83** erkannt und dieser Tastendruck im Schritt **84** verschlüsselt. Hierfür wird der zuvor befüllte Stack **90** herangezogen, von dem für jedes eingegebene Zeichen vom unteren Ende aus eine Schlüsselinformation genutzt und anschließend aus dem Stack **90** entfernt wird. Diese Schlüsselinformation wird genutzt, um den tatsächlich erfolgten Tastendruck **20** in einen anderweitigen Tastendruck **22** zu übertragen und somit zu verschlüsseln.

[0061] Der verschlüsselte Tastendruck **22** wird im Schritt **85** an die Zentraleinheit **60** weitergegeben, die dann diesen verschlüsselten Tastendruck **22** ohne die Möglichkeit der Entschlüsselung an die Gegenstelle **70** weitergibt. Da die Gegenstelle **70** einen identischen Stack **90** verwaltet, ist sie zur Entschlüsselung dieser Tastendruckinformationen in der Lage.

[0062] Die **Fig.** 5b verdeutlicht, wie die Verschlüsselung durch die Dekodier- und Enkodier-Einheit **62** und die anschließende Entschlüsselung durch die Gegenstelle **70** vonstattengeht.

[0063] Wenn das Wort PATENT durch den Benutzer an der Tastatur **68** eingegeben wird, so werden diese sechs Tastendrücke **20** nacheinander mit den Schlüsselinformationen im Stack **90** in Reihenfolge von deren vorherigem Eintreffen verschlüsselt. Statt die sechs Tastendrücke P, A, T, E, N, T an die Zentraleinheit **60** weiterzugeben, gibt die Dekodier- und Enkodier-Einheit **62** demnach die Tastendrücke R, V, H, L, Y, U weiter. Diese verschlüsselten Tastendrücke **22** sind zwar durch die Zentraleinheit **60** verarbeitbar und dementsprechend auch durch eine Trojaner-Software abgreifbar. Ohne die Schlüsselinfor-

mationen können diese Tastendrücke jedoch nicht in die ursprünglichen, tatsächlich stattgefundenen, überführt werden. Dies gelingt erst der Gegenstelle **70**, die die Schlüsselinformationen des Stacks **90** kennt.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102008062872 A1 [0002]

Patentansprüche

1. Verfahren zur Verschlüsselung von Tastendrücken (**20**), gekennzeichnet durch folgende Merkmalen:
a. ein Videodatenstrom wird analysiert und aus Bildinformationen (**50**) des Videodatenstroms eine Schlüsselinformation (**53c**, **90**) zur Verschlüsselung von Tastendrücken (**20**) ermittelt,
b. über einen Tastatureingangsanschluss werden erfolgte Tastendrücke (**20**) an einer angeschlossenen Tastatur (**68**) erfasst,
c. die erfassten Tastendrücke (**20**) werden unter Nutzung einer der Schlüsselinformationen (**53c**, **90**) verschlüsselt, so dass verschlüsselte Tastendrücke (**22**) erzeugt werden,
d. über einen Tastaturausgangsanschluss werden die verschlüsselten Tastendrücke (**22**) an eine Zentraleinheit weitergegeben.

2. Verfahren nach Anspruch 1 mit den Merkmalen:
a. bei der Verschlüsselung der erfassten Tastendrücke (**20**) findet eine Verschiebungs-Verschlüsselung unter Nutzung eines Verschiebungswertes Anwendung, und
b. der Verschiebungswert ist Teil der im Videodatenstrom enthaltenen Schlüsselinformationen (**53c**, **90**).

3. Verfahren nach Anspruch 1 oder 2 mit dem Merkmal:
a. die Schlüsselinformationen (**53c**, **90**) zur Verschlüsselung von Tastendrücken (**20**) liegt im Videodatenstrom in verschlüsselter Form vor.

4. Verfahren nach einem der Ansprüche 1 bis 3 mit dem Merkmal:
a. die Schlüsselinformationen (**53c**, **90**) zur Verschlüsselung von Tastendrücken (**20**), die aus dem Videodatenstrom ermittelt wird, umfasst eine Mehrzahl von nacheinander zu verwendenden Einzelschlüsselinformationen, die gemeinsam in einem gemeinsamen Einzelbild (**50**) des Videodatenstroms enthalten sind.

5. System zur Verschlüsselung von Tastaturdaten mit den folgenden Merkmalen:
a. das System verfügt über eine Video-Dekodier-Einheit (**62**) mit einem Videoeingangsanschluss,
b. das System verfügt über eine Tastatur-Enkodier-Einheit (**62**) mit einem Tastatureingangsanschluss zum Anschließen einer Tastatur (**68**) und einem Tastaturausgangsanschluss zum Anschließen an eine Zentraleinheit (**60**),
c. das System ist zur Durchführung des Verfahrens nach Anspruch 1 ausgebildet.

6. System nach Anspruch 5 mit dem Merkmal:
a. die Video-Dekodier-Einheit (**62**) und die Tastatur-Enkodier-Einheit (**62**) sind Teil eines gemeinsamen Gerätes.

7. System nach Anspruch 5 mit dem Merkmal:
a. die Video-Dekodier-Einheit und die Tastatur-Enkodier-Einheit sind als getrennte Einheiten ausgebildet, die über eine Kabelverbindung miteinander verbunden sind.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

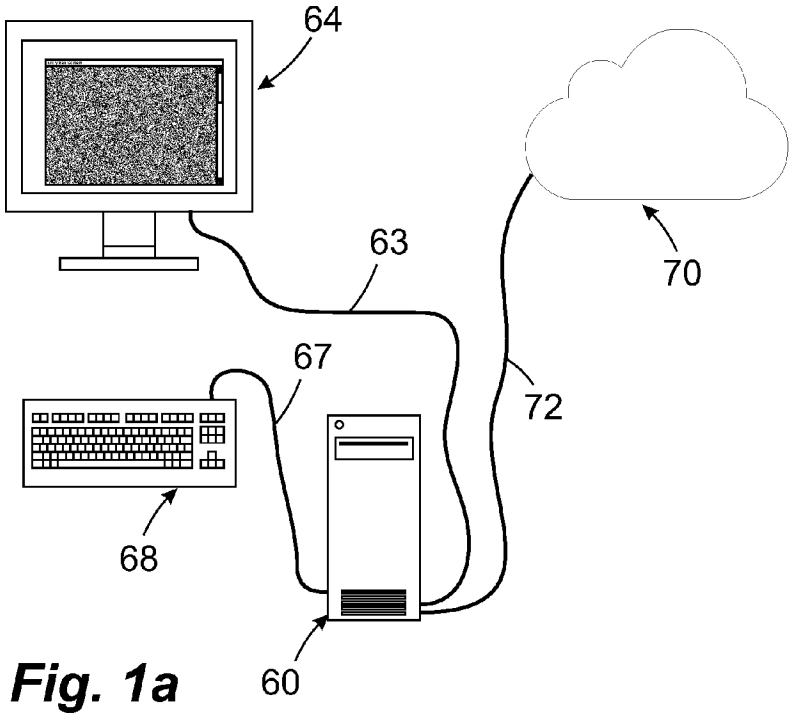


Fig. 1a

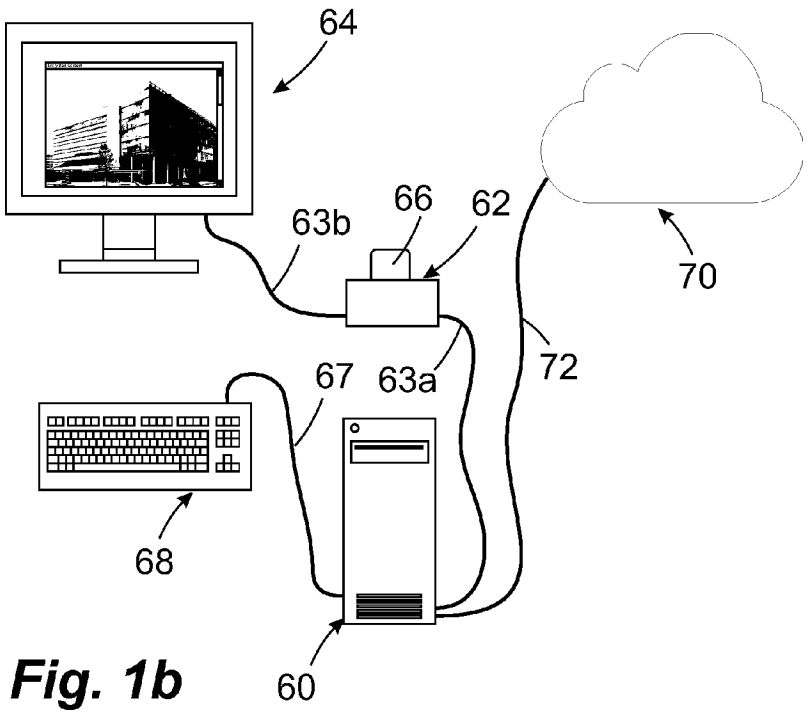


Fig. 1b

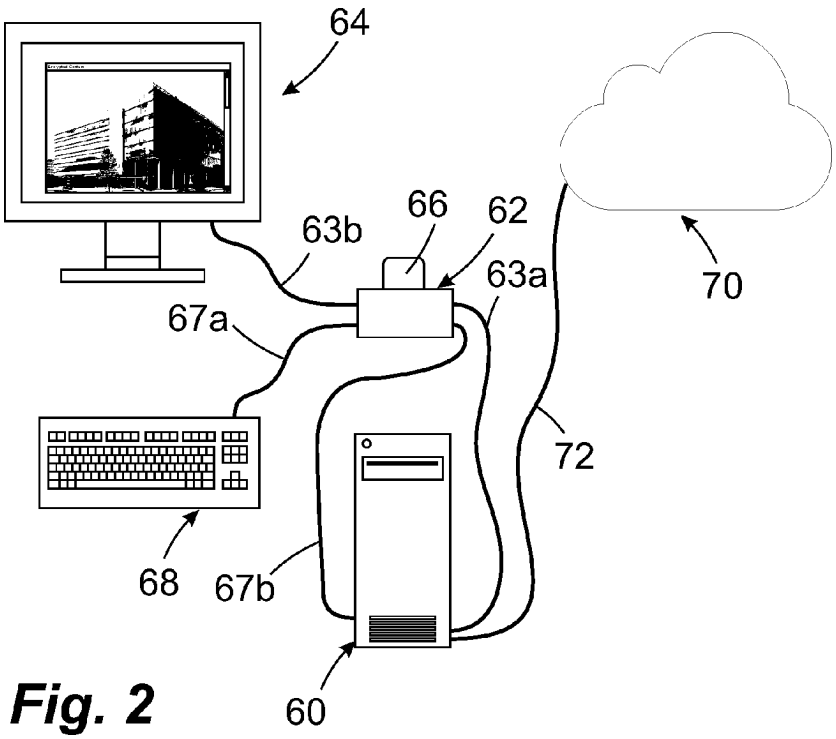


Fig. 2

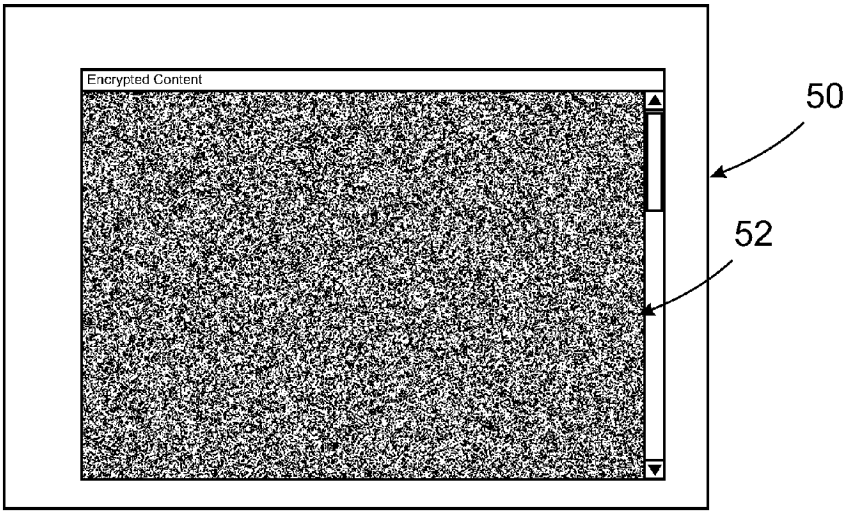


Fig. 3a

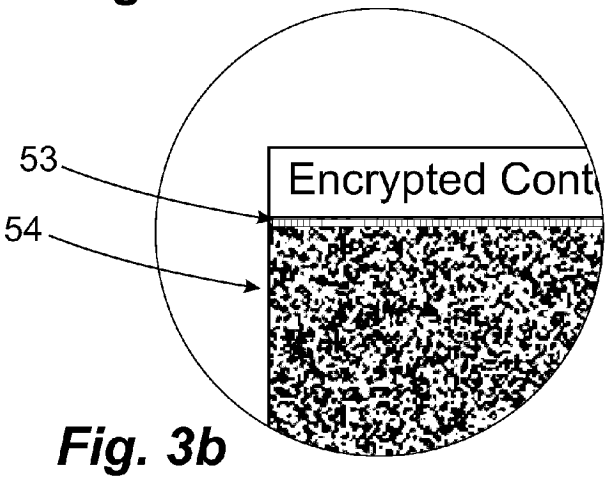


Fig. 3b

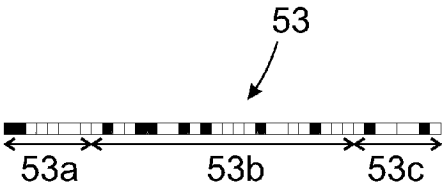


Fig. 3c

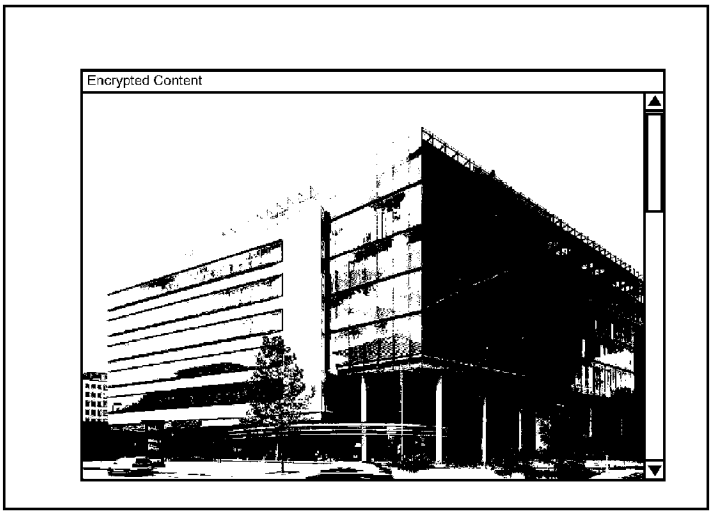


Fig. 3d

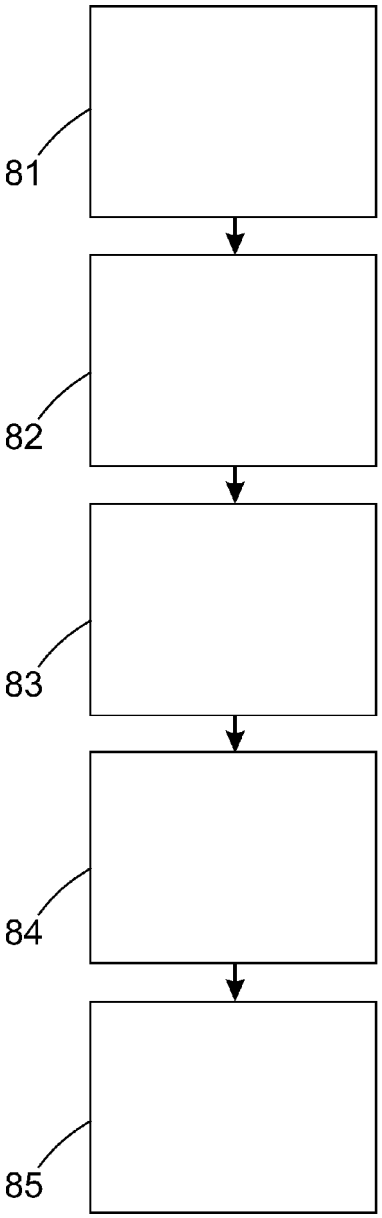


Fig. 4

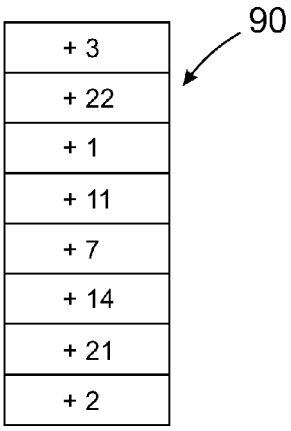


Fig. 5a

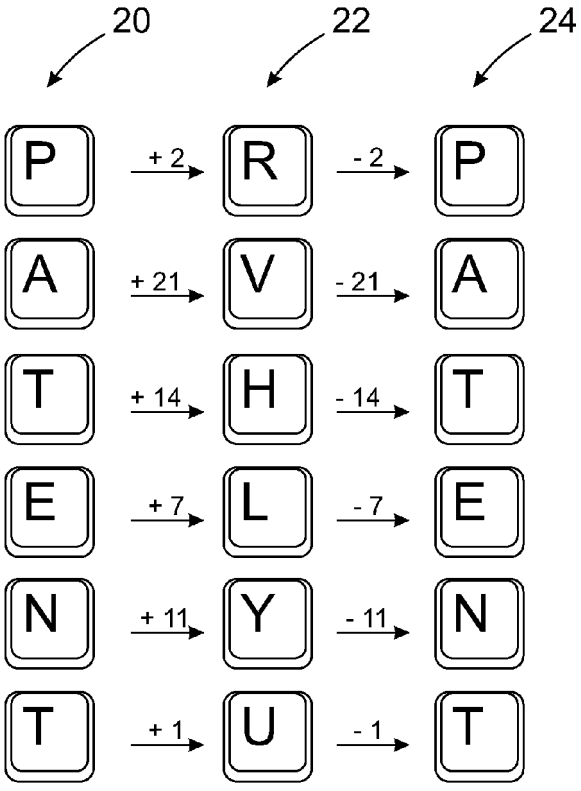


Fig. 5b