(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 103 121 B4** 2018.01.11

(12) # Patentschrift

(21) Aktenzeichen: **10 2015 103 121.3**
(22) Anmeldetag: **04.03.2015**
(43) Offenlegungstag: **08.09.2016**
(45) Veröffentlichungstag der Patenterteilung: **11.01.2018**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
G06F 21/60 (2013.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
Sultani, Omid, 20099 Hamburg, DE

(74) Vertreter:
Reichert & Lindner Partnerschaft Patentanwälte, 93047 Regensburg, DE

(72) Erfinder:
gleich Patentinhaber

(56) Ermittelter Stand der Technik:

US	**2014 / 0 229 544**	**A1**
WO	**2012/ 087 646**	**A2**

(54) Bezeichnung: **VERFAHREN UND SYSTEM ZUR COMPUTERGESTÜTZTEN SICHEREN KOMMUNIKATION ZWISCHEN DATENVERARBEITUNGSEINHEITEN**

(57) Hauptanspruch: Verfahren zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit (2) eines Versenders (V) und mindestens einer Datenverarbeitungseinheit (2_1, 2_2, ..., 2_N) eines ausgewählten Kontakts (K1, K2, ..., KN) gekennzeichnet durch die folgenden Schritte:

• dass ein Anwendungsprogramm gestartet wird;

• dass von einem Versender (V) ein alphanumerischer und/oder bildlicher Datensatz (10) ausgewählt wird, der vom Versender (V) an mindestens einen aus einer Kontaktliste (30) ausgewählten Kontakt (K1, K2, ..., KN) versendet wird;

• dass dem mindestens einen ausgewählten Kontakt (K1, K2, ..., KN) eine Berechtigung (15) vom Versender (V) zugewiesen wird, wobei die Datenverarbeitungseinheit (2) des Versenders (V) mit einem Server (40) kommuniziert, so dass die Berechtigung (15) auf dem Server (40) gespeichert wird;

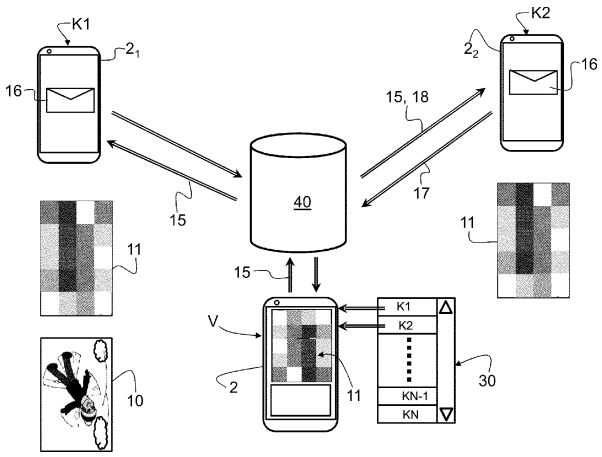
• dass der ausgewählte alphanumerische und/oder bildliche Datensatz (10) vor dem Versenden an den mindestens einen ausgewählten Kontakt (K1, K2, ..., KN) verpixelt und als verpixelter Datensatz (11) an eine Datenverarbeitungseinheit (2_1, 2_2, ..., 2_N) des mindestens einen Kontakts (K1, K2, ..., KN) übermittelt wird;

• dass die Datenverarbeitungseinheit (2_1, 2_2, ..., 2_N) des mindestens einen ausgewählten Kontakts (K1, K2, ..., KN) mit den Server (40) kommuniziert und die Berechtigung (15) abfragt;

• dass bei Berechtigung (15) des Kontakts die Verpixelung des vom Versender (V) versendeten und verpixelten Datensatzes (11) entfernt wird;

• dass falls ein von einem berechtigten Kontakt (K1, K2, ..., KN) angefertigter Screenshot (22) des empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatzes (10) zumindest teilweise unkenntlich gemacht wird und/oder mit einer Kennung (26) des berechtigten Kontakts (K1, K2, ..., KN) versehen wird; und

• dass falls ein von der Datenverarbeitungseinheit (2_1, 2_2, ..., 2_N) eines berechtigten Kontakts (K1, K2, ..., KN) ein alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz (10) mit einer weiteren Datenverarbeitungseinheit (2_1, 2_2, ..., 2_N) abfotographiert wird, der alphanumerische und/oder bildliche und nicht verpixelte Datensatz mit einer Kennung (26) versehen wird.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur computergestützten, sicheren und kontrollierten Kommunikation zwischen mindestens zwei Datenverarbeitungseinheiten.

[0002] Ferner betrifft die Erfindung ein System zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit als Versender und mindestens einer weiteren Datenverarbeitungseinheit als Empfänger.

[0003] Die deutsche Patentanmeldung DE 10 2010 060 282 offenbart ein Verfahren zur computergestützten Kommunikation. Die computergestützte Kommunikation läuft dabei insbesondere über das Internet, mit welcher mindestens zwei Nutzer Nachrichten austauschen und dabei Bilder des jeweils anderen Benutzers angezeigt bekommen. Dabei ändert sich ein Erkennungsgrad der Bilder im Verlauf des Kommunikationsvorgangs. Nach einer gewissen Anzahl von ausgetauschten Nachrichten ist die Erkennbarkeit größer als 0 % und kleiner als 100 %. Das Maß des Kennenlernens bzw. des Vertrauens-Aufbaus regelt das Maß der Erkennbarkeit. Die beiden Nutzer sind mittels eines Servers verbunden. Dieses System kann keine sichere Kommunikation zwischen mobilen Endgeräten oder Datenverarbeitungseinheiten gewährleisten. Alphanumerische und/oder bildliche Datensätze können hiermit nicht derart versendet werden, damit eine Sicherheit vor einem Zugriff anderer, nicht berechtigter Benutzer, gewährleistet ist.

[0004] Das U.S.-Patent US 8,744,143 beschreibt ein Verfahren, mit dem ein Schutz der Privatsphäre hochgeladener Bilder möglich ist. Hierzu wird eine Person in einem aufgenommenen Bild identifiziert. Ein Teil des Bildes, der die Person zeigt, wird verschwommen dargestellt, um eine Erkennbarkeit der Person zu vermeiden. Die Person wird mit einem Schild (Tag) versehen. Die Unkenntlichmachung wird nur dann entfernt, wenn eine Zustimmung dem Freund (bzw. anderen Nutzer) gegenüber erteilt wird. Die Zustimmung kann z. B. dadurch erreicht werden, dass eine Nachricht an die mit dem Schild (Tag) versehene, nicht erkennbare Person versendet wird. Nach der Zustimmung können andere Freunde oder die Öffentlichkeit des sozialen Netzwerks das Bild sehen oder herunterladen. Falls keine Zustimmung zurückgesendet wird, bleibt das Bild weiterhin verschwommen.

[0005] Die U.S.-Patentanmeldung US 2012/0219053 offenbart eine Vorrichtung zum Übertragen von Daten, wobei die Übertragung mittels eines verschlüsselten Bildes erfolgt. Hierzu ist ein Kommunikationssystem mit einer ersten Einheit und einer zweiten Einheit offenbart. Die erste Einheit umfasst einen Speicher, der die Daten speichert, die an die zweite Einheit übertragen werden sollen. Auf einem Display der ersten Einheit kann das zu übertragende und kodierte Bild dargestellt werden. Die Kamera der zweiten Einheit ist zur Aufnahme des dargestellten Bildes auf das Display der ersten Einheit hin ausgerichtet. Die zweite Einheit sendet eine Statusmeldung an die erste Einheit, wie z. B. den Erfolg der Decodierung. Diese Übertragungsmethode resultiert zwar in einer hohen Datensicherheit, jedoch müssen die erste Einheit und die zweite Einheit zueinander ausgerichtet sein.

[0006] Die U.S.-Patentanmeldung US 2014/0258707 A1 offenbart ein sicheres Kommunikationssystem zwischen mobilen Geräten. Es ist eine direkte Kommunikation zwischen einem sendenden mobilen Gerät und einem empfangenden mobilen Gerät beschrieben. Das sendende Gerät fordert vom empfangenden Gerät einen öffentlichen Schlüssel an. Mit dem öffentlichen Schlüssel wird die zu übertragende Datei verschlüsselt. Die verschlüsselte Datei kann als Anhang zu einer Nachricht übertragen werden. Das empfangende Gerät kann mit einem privaten Schlüssel und dem zuvor empfangenen öffentlichen Schlüssel die Datei entschlüsseln. Selbst wenn ein drittes mobiles Gerät die verschlüsselte Datei und den öffentlichen Schlüssel abfängt, so fehlt zur Entschlüsselung beim dritten Gerät der private Schlüssel.

[0007] Die U.S.-Patentanmeldung US 2011/0149014 A1 offenbart eine Kommunikationseinrichtung und ein Verfahren zum Schutz der Privatsphäre. Das Mobiltelefon kann während einer Kommunikation benutzt werden, um die Privatsphäre des Angerufenen zu schützen. Hierzu besitzt das Mobiltelefon eine spezielle Einheit. Mit der Kamera können Bilder oder Videos aufgenommen werden. Das im Mobiltelefon installierte Programm kann dazu verwendet werden, um die Privatsphäre während des Videoanrufs zu schützen. Wenn das Mobiltelefon angerufen wird, wird eine Dialogbox auf dem Display erzeugt, mit der die Freigabe für eine Videoübertragung oder die Übertragung eines im Speicher abgelegten Bildes freigegeben wird. Eine Unkenntlichmachung der übertragenen alphanumerischen und/oder bildlichen Daten ist nicht vorgesehen.

[0008] Die britische Patentanmeldung GB 25 12 140 A offenbart ein System und eine Methode zur Nachrichtenübermittlung. Es ist ein sicheres Verfahren offenbart, um feststellen zu können, ob ein Screenshot von einem Empfänger eine Nachricht gemacht wurde. Ebenso wird verhindert, dass Screenshots mit einer externen Kamera gemacht werden können. Hierzu kann z. B. das Bild mit einem Wasserzeichen versehen werden. Hiermit sind das unerlaubte Aufnehmen von Screenshots und damit das Verbreiten derselben erschwert. Es ist jedoch nicht möglich, dass hiermit auch alphanumerische und/oder

bildliche Datensätze sicher und nicht für jeden Dritten lesbar übermittelt werden können.

[0009] Die japanische Patentanmeldung JP 2014/089625 offenbart ein Verfahren zum Suchen eines Menschen unter Berücksichtigung der Privatsphäre. Mit einem Such-String kann nach Gesichtern von Personen gesucht werden, die auf Bildern im Internet dargestellt sind und dies erlaubt haben. Bei Personen, die nicht die Erlaubnis erteilt haben, wird das Gesicht zum Schutze der Privatsphäre unkenntlich gemacht.

[0010] Die internationale Patentanmeldung WO 2013/160539 offenbart ein Verfahren und eine Vorrichtung zum Schutze der Privatsphäre in Bildern. Hierzu wird auf einem Server die erste Einstellung eines Benutzers bzgl. der Privatsphäre gespeichert. Mit der ersten Einstellung wird das Gesicht eines Benutzers erkannt. Die zweite Einstellung wird an einen zweiten Benutzer eines zweiten mobilen Gerätes gesendet. Nach einer bestimmten Zeit wird ein Teil des Bildes verschwommen dargestellt. Eine sofortige Versendung von alphanumerischen und/oder bildlichen Datensätzen, die bereits beim Versenden unkenntlich gemacht worden sind, ist hier nicht offenbart.

[0011] Das U.S.-Patent 8,914,752 offenbart ein Verfahren zum Versenden von Nachrichten. Die versendeten Nachrichten werden nach einer Zeitspanne nach dem ersten Betrachten automatisch gelöscht. Eine Berührung des Displays des mobilen Geräts setzt einen Timer in Gang, der die Zeitspanne vorgibt. Nach Ablauf dieser Zeitspanne wird die übermittelte Nachricht gelöscht.

[0012] Die internationale Patentanmeldung WO 2014/194262 offenbart einen Server mit einem Modul für Nachrichten. Dabei werden von einem Prozessor Anweisungen ausgeführt, um eine Nachricht zwischen einem ersten Benutzer und einem zweiten Benutzer aufrechtzuerhalten. Jeder Eintrag in die Nachricht wird nach einer vorbestimmten Zeit gelöscht, es sei denn, dass eine andere Anweisung eintrifft.

[0013] Das U.S.-Patent US 8,909,725 B1 offenbart ein Servermodul, das Push-Kriterien ermittelt. Anhand der Push-Kriterien werden Objekte (Bilder mit Text, Bilder oder Videos) an einen oder mehrere Edge-Server gesendet, so dass die Anfrage eines Benutzers befriedigt wird. Es könnten dann auch Lösch-Kriterien festgelegt werden, wie z. B. dass nach einem einmaligen Betrachten das Objekt gelöscht wird.

[0014] Die U.S.-Patentanmeldung US 2013/0305383 A1 offenbart ein System und Verfahren zum Schutz der Privatsphäre der von Nutzern auf Internetseiten hochgeladenen Multimedia-Daten. Ein Server, auf dem ein Internet-Datenschutzdienst implementiert ist, empfängt ein Medienelement eines Nutzers des sozialen Netzwerks. Das Medienelement (z. B. Bild) wird verschlüsselt. Eine Vereinbarung bestimmt, wer das Medienelement sehen kann. Die verschlüsselten Medienelemente werden sicher in einer Cloud gespeichert. Die verschlüsselten Bilder sind mittels DRM-Schutz und Zugangskontrolle gesichert. Ein Benutzer mit Zugangsrecht kann das Bild herunterladen und es kann nach der Entschlüsselung betrachtet werden.

[0015] Die US-Patentanmeldung US 2014/0229544 A1 offenbart ein Verfahren zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit eines sozialen Netzwerks. Hierzu ist auf den Datenverarbeitungseinheiten ein Anwendungsprogramm installiert. Von einem Versender wird ein bildlicher Datensatz ausgewählt, der mit den ausgewählten Kontakten einer Kontaktliste geteilt werden soll. Den ausgewählten Kontakten wir zum Betrachten der Datensätze eine Berechtigung zugewiesen, die auf einen Server verwaltet wird. Die Datensätze liegen zunächst verpixelt vor und nur die ausgewählten Kontakte können den Inhalt unverpixelt mittels der Berechtigung betrachten.

[0016] Die internationale Patentanmeldung WO 2012/087646 offenbart ein Verfahren zum Schutz der Nutzerprivatsphäre in sozialen Netzwerken. Hierzu werden aus Bildern mit voller Auflösung sogenannte Proxy-Bilder bzw. verkleinerte, unkenntlich gemachte Bilder erzeugt und diese zunächst einem zugreifenden Benutzer anzeigt. Nachdem dieser Benutzer berechtigt ist die volle Auflösung zu sehen, werden diese Bilder dem Benutzer angezeigt.

[0017] Weder WhatsApp, Facebook, Skype oder Snapchat stellen eine Möglichkeit zur Verfügung, mittels der alphanumerische und/oder bildliche Datensätze derart versendet werden, dass ein Dritter den Inhalt der Datensätze nicht erkennen kann. Erst bei einer Berechtigung von dem Versender kann der Empfänger den alphanumerischen und/oder bildlichen Datensatz auf seiner Datenverarbeitungseinheit betrachten.

[0018] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur computergestützten, sicheren Kommunikation zwischen Datenverarbeitungseinheiten zu schaffen, mit der Nachrichten, Bilder, Tonaufnahmen und Videos verschlüsselt gesendet und wiederum empfangen werden können. Ebenso soll eine ungehinderte Verbreitung dieser Nachrichten vermieden werden.

[0019] Diese Aufgabe wird durch ein Verfahren gelöst, das die Merkmale des Anspruchs 1 umfasst.

[0020] Ferner ist es Aufgabe der Erfindung, ein nicht flüchtiges computerlesbarer Speichermedium bereitzustellen, das computerlesbare Anweisungen umfasst, mit denen es möglich ist, Nachrichten zwischen mindestens zwei Datenverarbeitungseinheiten derart auszutauschen, das ein Dritter die Nachricht nicht lesen kann und der Empfänger der Nachricht diese ebenfalls nur lesen kann, wenn er hierzu eine Berechtigung hat.

[0021] Diese Aufgabe wird durch ein nicht flüchtiges computerlesbares Speichermedium gelöst, das die Merkmale des Anspruchs 7 umfasst.

[0022] Eine weitere Aufgabe der Erfindung ist, ein System zur computergestützten, sicheren und kontrollierten Kommunikation zwischen Datenverarbeitungseinheiten zu schaffen, wobei auf einfache Weise sichergestellt werden kann, dass übermittelte alphanumerische und/oder bildliche Datensätze von einem nicht Berechtigten nicht gelesen werden können.

[0023] Diese Aufgabe wird durch ein System gelöst, das die Merkmale des Anspruchs 12 umfasst.

[0024] Das Verfahren zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit eines Senders und mindestens einer Datenverarbeitungseinheit eines ausgewählten Kontakts zeichnet sich durch die folgenden Schritte aus:

- dass ein Anwendungsprogramm gestartet wird;
- dass von einem Versender ein alphanumerischer und/oder bildlicher Datensatz ausgewählt wird, der vom Versender an mindestens einen aus einer Kontaktliste ausgewählten Kontakt versendet wird;
- dass dem mindestens einen ausgewählten Kontakt eine Berechtigung vom Versender zugewiesen wird, wobei die Datenverarbeitungseinheit des Senders mit einem Server kommuniziert, so dass die Berechtigung auf dem Server gespeichert wird;
- dass der ausgewählte alphanumerische und/oder bildliche Datensatz vor dem Versenden an den mindestens einen ausgewählten Kontakt verpixelt und als verpixelter Datensatz an eine Datenverarbeitungseinheit des mindestens einen Kontakts übermittelt wird;
- dass die Datenverarbeitungseinheit des mindestens einen ausgewählten Kontakts mit dem Server kommuniziert und die Berechtigung abfragt;
- dass die Berechtigung des Kontakts die Verpixelung des vom Versender versendeten verpixelten Datensatzes entfernt wird;
- dass falls ein von einem berechtigten Kontakt angefertigter Screenshot des empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatzes zumindest teilweise unkenntlich gemacht wird und/oder mit einer Kennung des berechtigten Kontakts versehen wird; und
- dass falls ein von der Datenverarbeitungseinheit eines berechtigten Kontakts ein alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz mit einer weiteren Datenverarbeitungseinheit abfotographiert wird, der alphanumerische und/oder bildliche und nicht verpixelte Datensatz mit einer Kennung versehen wird.

[0025] Der versendete und verpixelte Datensatz kann mit einem Logo des Anwendungsprogramms versehen werden. Wobei das Logo einen berechtigten Kontakt anzeigt, dass zum nicht verpixelten Betrachten des empfangenen und verpixelten Datensatzes zuerst das Anwendungsprogramm auf die Datenverarbeitungseinheit geladen werden muss.

[0026] Dieses Konzept hat den Vorteil, dass mit dem Anwendungsprogramm Nachrichten, Bilder, Tonaufnahmen und Videos verschlüsselt gesendet und wiederum empfangen werden können. Für das nicht verschlüsselte Betrachten der versendeten Datensätze ist es erforderlich, dass das entsprechende Anwendungsprogramm auf der zugehörigen Datenverarbeitungseinheit geladen ist. Ebenso ist sichergestellt, falls ein nicht berechtigter Kontakt den Datensatz empfängt, er mit diesem Datensatz nichts anfangen kann, da er nicht die Verschlüsselung bzw. Verpixelung vom gesendeten Datensatz entfernen kann. Ebenso bringt eine weitere Verbreitung der versendeten und verpixelten Datensätze durch den nicht berechtigten Kontakt für ihn keinen Vorteil, da ebenfalls ein weiterer Empfänger diesen versendeten und verpixelten Datensatz nicht entschlüsseln bzw. unverpixelt betrachten kann.

[0027] Ebenso kann ein nicht berechtigter Kontakt, der einen verpixelten Datensatz empfangen hat, eine Nachricht an den Versender senden, um eine Berechtigung für das nicht verpixelte Betrachten des empfangenen alphanumerischen und/oder bildlichen Datensatzes zu erhalten. Für den Fall, dass der Versender dem nicht berechtigten Kontakt eine Berechtigung erteilt, wird dies vom Versender dem Server mitgeteilt. Über den Server erhält dann der vormals nicht berechtigte Kontakt die Berechtigung den alphanumerischen und/oder bildlichen Datensatz nicht verpixelt zu betrachten.

[0028] Ebenso ist es gemäß einer Ausführungsform des erfindungsgemäßen Verfahrens möglich, einen Screenshot des empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatzes durch einen berechtigten Kontakt zu verhindern. Für den Fall, dass von einem berechtigten Kontakt ein entsprechender Screenshot angefertigt wird, wird dieser zumindest teilweise unkenntlich gemacht. Parallel dazu kann der Screenshot auch mit einer Kennung des berechtigten Kontakts versehen

werden. Dies hat den Vorteil, falls ein nicht verpixelter Datensatz mit der entsprechenden Kennung im Internet oder in entsprechenden sozialen Netzwerken auftaucht, dieser nicht verpixelte Datensatz eindeutig einer Person zugewiesen werden kann. Diesen berechtigten Kontakt die Berechtigung entzogen werden, was am zentralen Server gemacht werden kann. Ein Hinweis hierzu kann z. B. auch in den AGB's für die Benutzung des erfindungsgemäßen Anwendungsprogramms niedergelegt sein.

[0029] Ferner kann es vorkommen, dass ein von der Datenverarbeitungseinheit eines berechtigten Kontakts empfangener alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz mit einer weiteren Datenverarbeitungseinheit abfotografiert wird. Bei dem Abfotografieren wird der alphanumerische und/oder bildliche Datensatz ebenfalls mit einer Kennung versehen und wie bereits oben erwähnt, kann ggf. dem vormals berechtigten Kontakt die Berechtigung entzogen werden.

[0030] Die von dem mindestens einen berechtigten Kontakt empfangenen alphanumerischen und/oder bildlichen Datensätze werden in einem dem Anwendungsprogramm zugewiesenen Album gespeichert. Dabei ist es immer so, dass ein Versenden des empfangenen alphanumerischen und/oder bildlichen Datensatzes verpixelt erfolgt und keine weiteren Berechtigungen zugewiesen werden, als diejenigen, die bereits vom ursprünglichen Versender vergeben worden sind.

[0031] Die Datenverarbeitungseinheiten sind bevorzugt als mobile Geräte ausgebildet.

[0032] Ebenso kann ein nicht flüchtiges computerlesbares Speichermedium vorgesehen sein, das computerlesbare Anweisungen umfasst, die auf dem Speichermedium gespeichert sind. Die computerlesbaren Anweisungen sind auf mindestens einem Prozessor mindestens einer Datenverarbeitungseinheit des Versenders und auf mindestens einem Prozessor einer Datenverarbeitungseinheit mindestens eines Kontakts ausführbar. Dieses Anwendungsprogramm ermöglicht eine computergestützte, sichere und kontrollierbare Kommunikation mit mindestens einer Datenverarbeitungseinheit mindestens eines weiteren Kontakts. Ebenso ist dadurch die unkontrollierte Verbreitung von alphanumerischen und/oder bildlichen Datensätzen eingeschränkt. Ein vom Versender ausgewählter alphanumerischer und/oder bildlicher Datensatz wird vor dem Versenden an den mindestens einen ausgewählten Kontakt als ein verpixelter Datensatz auf einem Display der Datenverarbeitungseinheit des Versenders dargestellt. Der Versender wählt dabei mindestens einen Kontakt aus einer Kontaktliste aus, an den der verpixelte Datensatz versendet wird. Eine Berechtigung wird vom Versender an einen zentralen Server übermittelt und dort gespeichert. Die Berechtigung zeigt an, dass der mindestens eine ausgewählte Kontakt den alphanumerischen und/oder bildlichen Datensatz nicht verpixelt betrachten kann. Nach dem Empfangen einer Nachricht des Versenders, dass ein verpixelter Datensatz gesendet wurde, kommuniziert die Datenverarbeitungseinheit des mindestens einen ausgewählten Kontakts mit dem Server und fragt die Berechtigung ab. Die Berechtigung wird von dem Server in Echtzeit überprüft und falls die Berechtigung vorliegt, kann der Kontakt die Verpixelung des vom Versender versendeten und verpixelten Datensatzes entfernen.

[0033] Die computerlesbaren Anweisungen auf dem nicht flüchtigen computerlesbaren Speichermedium ermöglichen es ebenfalls, dass der versendete und verpixelte Datensatz mit einem Logo eines aus dem computerlesbaren Anweisungen bestehenden Anwendungsprogramms versehen werden kann. Das Logo zeigt dabei einen berechtigten Kontakt an, dass zum nicht verpixelten Betrachten des empfangen verpixelten Datensatzes zuerst das Anwendungsprogramm auf die Datenverarbeitungseinheit geladen werden muss.

[0034] Das System zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit als Versender und mindestens einer weiteren Datenverarbeitungseinheit als Empfänger umfasst einen Server, mit dem die Datenverarbeitungseinheit des Versenders und die mindestens eine weitere Datenverarbeitungseinheit kommunikativ verbunden sind. Ferner ist ein Prozessor der Datenverarbeitungseinheit des Versenders vorgesehen, auf dem ein Anwendungsprogramm ausführbar ist. Das Anwendungsprogramm erstellt aus einem alphanumerischen und/oder bildlichen Datensatz einen verpixelten Datensatz. Über ein Eingabemittel der Datenverarbeitungseinheit des Versenders kann mindestens ein Kontakt ausgewählt werden, an den der verpixelte Datensatz gesendet wird. Dieser ausgewählte Kontakt ist somit auch zum Betrachten des alphanumerischen und/oder bildlichen Datensatzes ohne Verpixelung berechtigt. Die Berechtigung ist von der Datenverarbeitungseinheit des Versenders auf dem Server hinterlegt worden. Ein Prozessor der mindestens einen weiteren Datenverarbeitungseinheit, auf dem ebenfalls das Anwendungsprogramm ausführbar ist, stellt aus dem verpixelten Datensatz den alphanumerischen und/oder bildlichen Datensatz wieder her. Zur Ausführung des Anwendungsprogramms mit der weiteren Datenverarbeitungseinheit des mindestens einen Kontakts muss vorher die Berechtigung vom Server abgerufen bzw. angefragt werden.

[0035] Obwohl sich die nachfolgende Beschreibung ausschließlich auf mobile Geräte als Datenverarbeitungseinheit beschränkt, soll dies nicht als eine Beschränkung der Erfindung aufgefasst werden. Es ist

für einen Fachmann selbstverständlich, dass die Erfindung bei unterschiedlichen Datenverarbeitungseinheiten implementiert werden kann.

[0036] Das erfindungsgemäße Anwendungsprogramm (APP) soll hauptsächlich auf mobilen Geräten (Smartphones) laufen. Das Anwendungsprogramm läuft unter iOS (Apple) und Android-Betriebssystemen. Darüber hinaus umfasst das Anwendungsprogramm auch die Grundfunktionen von WhatsApp. Benutzer bzw. Kontakte können mit dem Anwendungsprogramm Nachrichten versenden und auch empfangen. Das Ganze wird über eine Server-Umgebung realisiert. Benutzer bzw. Kontakte können über einen Balken sehen, ob ein anderer Kontakt online ist, oder ob er gerade schreibt.

[0037] Eine weitere Möglichkeit des erfindungsgemäßen Anwendungsprogramms ist, das ein Benutzer eine Nachricht schreiben kann und letztendlich bestimmt, um welche Uhrzeit diese Nachricht für einen anderen Nutzer bzw. Kontakt sichtbar wird. Hierzu wird ein Timer eingestellt, der festlegt, dass die Nachricht erst zu einer bestimmten Uhrzeit versendet wird und somit für den anderen Nutzer bzw. Kontakt sichtbar wird. Ebenso ist es möglich, dass die Nachricht erst zu einem bestimmten Zeitpunkt für den zweiten Benutzer sichtbar wird.

[0038] Das Anwendungsprogramm hat den Vorteil, dass verschlüsselte Nachrichten versendet werden können. Die Nachrichten können Textnachrichten, Bilder, Tonaufnahmen und Videos sein, die verschlüsselt versendet und ebenfalls wieder verschlüsselt empfangen werden können. Ebenso wird das Anwendungsprogramm eine ähnliche Funktion wie Facebook haben. Das Anwendungsprogramm wird ein Fotoalbum besitzen. Dort kann man die Fotos kommentieren. Ebenso wird das Anwendungsprogramm eine Pinnwand umfassen. Die Benutzer des Anwendungsprogramms können ihre Profile gestalten und mit Informationen füllen. Ebenso kann zu Homepages dazu anordnen.

[0039] Wie bereits erwähnt, ist es möglich, mit dem erfindungsgemäßen Anwendungsprogramm Nachrichten verschlüsselt zu versenden. Bei dem erfindungsgemäßen Anwendungsprogramm wird die Verschlüsselung dadurch erreicht, dass die Nachrichten verpixelt sind und somit nicht für jeden Dritten lesbar.

[0040] Die Nachrichten werden also verpixelt versendet. Vor dem verpixelten Versenden kann der Versender bestimmte Freigaben in seiner eigenen Kontaktliste erteilen. Diese Freigaben bzw. Berechtigungen werden an den Server übermittelt. Mit Hilfe der Freigabefunktion kann man seine persönliche Information vor anderen Usern (nicht berechtigten Kontakten) schützen. Bevor die Nachricht aus dem Anwendungsprogramm heraus versendet wird, fragt das Anwendungsprogramm wer die Erlaubnis (Freigabe) hat, die Nachricht unverpixelt zu sehen. Nachdem man die Personen (Kontakte) ausgewählt hat, kann die Nachricht versendet werden, ohne dass die Gefahr besteht, dass Unberechtigte diese Nachricht lesen. Personen, die das Anwendungsprogramm nicht auf ihren mobilen Geräten haben, werden auch nur ein verpixeltes Bild der Nachricht sehen können. Das Versenden und die Freigabe zum nicht verpixelten Betrachten der verpixelten Nachrichten werden in Echtzeit auf einem Hochleistungsserver berechnet, der mit den mobilen Geräten kommuniziert. Gemäß einer weiteren Ausgestaltung des Anwendungsprogramms ist es möglich, dass Nachrichten mit einem Abfalldatum versehen werden. Benutzer können durch die Option wählen und bestimmen, wie lange eine versendete Nachricht (Video oder Bild) und andere persönliche Informationen für einen anderen Nutzer sichtbar bleiben. Nach Ablauf der Zeit wird das Bild, Video und die persönliche Information automatisch gelöscht.

[0041] Um sicherzugehen, dass eine Verbreitung von versendeten Bildern, Nachrichten, Videos und dergleichen nicht möglich ist, muss verhindert werden, dass Screenshots ohne Kontrolle von den aus dem Anwendungsprogramm versendeten Nachrichten gemacht werden. Für den Fall, dass ein User einen Screenshot mit seinem mobilen Gerät macht gemacht hat, wird gemäß einer möglichen Ausführungsform automatisch ein schwarzes Bild gespeichert. Ebenso ist es möglich, dass das Bild mit graphischen Elementen unkenntlich gemacht wird. Parallel zum Unkenntlichmachen des Bildes bzw. der Nachricht, können ebenfalls Kontaktdaten des Users, der den Screenshot angefertigt hat, auf dem Bild eingeblendet werden. Somit hat man die Möglichkeit, dass man einen Nutzer, der öfter gegen die AGB's des Anwendungsprogramms verstößt, von der Nutzung des Anwendungsprogramms auszuschließen. Für den Fall, dass mit einem weiteren mobilen Gerät die nicht verpixelte Nachricht von einem anderen mobilen Gerät abphotographiert wird, ist es möglich, dass an einem Bildschirmrand permanent ein Nutzername kzw andere Kontaktdaten angezeigt werden. Derartig abphotographierte Nachrichten oder Bilder können somit nur mit dem Nutzernamen weiterverbreitet werden. Für den Fall, dass man dies feststellt, kann ebenfalls dieser Nutzer von der Benutzung des Anwendungsprogramms ausgeschlossen werden.

[0042] Ebenso ist es sinnvoll, dass die verpixelten Nachrichten mit einem Logo des Anwendungsprogramms versehen werden, mit dem es möglich ist, die Nachricht nicht verpixelt zu betrachten. Ein Nutzer, der noch nicht dieses Anwendungsprogramm auf seinem mobilen Gerät hat, kann somit das Anwendungsprogramm herunterladen, damit er die verpixelte Nachricht, für den Fall das er eine Berechtigung hat, diese unverpixelt betrachten kann. Nachrichten,

die weiterverbreitet werden, werden immer mit Nutzerdaten versehen. Dies hat den Vorteil, dass ein Nutzer wiedererkannt und aufgefunden werden kann.

[0043] Ebenso ist es möglich, das Anwendungsprogramm mit einer Spielefunktion zu versehen. Nutzer haben die Möglichkeit z. B. Bilder zu mischen und als Puzzle zu teilen. Ein Nutzer kann somit einem anderen Nutzer ein Foto als Puzzle senden. Der Nutzer, der das Puzzle bekommt, kann es zusammensetzen und zurückschicken. Eine weitere Möglichkeit einer Spielefunktion ist, dass die Nutzer ein Bild sehen und danach werden Dinge aus dem Bild herausgenommen. Der Nutzer soll herausfinden, welche Dinge auf dem Bild fehlen. Die Dinge die fehlen könnten, werden als Werkzeugkasten am unteren Bildschirmrand des mobilen Geräts angezeigt. Nachdem man die fehlenden Dinge eingesetzt hat, wird man über ein Punktesystem belohnt. Dies alles soll nebenbei für mehr Unterhaltung sorgen.

[0044] Im Folgenden sollen die Ausführungsbeispiele die Erfindung und ihre Vorteile anhand der beigefügten Figuren näher erläutern. Die Größenverhältnisse in den Figuren entsprechen nicht immer den realen Größenverhältnissen, da einige Formen vereinfacht und andere Formen zur besseren Veranschaulichung vergrößert im Verhältnis zu anderen Elementen dargestellt sind. Es sei hier nochmals bemerkt, dass sich die nachstehende Beschreibung ausschließlich auf mobile Geräte (Smartphones) bezieht. Dies ist dabei keineswegs als Beschränkung der Erfindung aufzufassen.

[0045] Dabei zeigen:

[0046] Fig. 1 eine schematische Draufsicht auf ein mobiles Gerät (Smartphone);

[0047] Fig. 2 eine schematische Ansicht der Elemente eines mobilen Geräts;

[0048] Fig. 3 eine schematische Ansicht des Ablaufs des Versendens von Nachrichten von einem mobilen Gerät eines Versenders;

[0049] Fig. 4 eine schematische Ansicht des erfindungsgemäßen Systems, wobei mehrere mobile Geräte mit einem zentralen Server kommunizieren;

[0050] Fig. 5 eine schematische Ansicht des Ablaufs, bei dem ein Nutzer eine Berechtigung zum Betrachten von verpixelten Nachrichten hat;

[0051] Fig. 6 zeigt eine schematische Ansicht eines Ablaufs, bei dem ein berechtigter Benutzer das für das nicht verpixelte Betrachten der Nachrichten erforderliche Anwendungsprogramm noch nicht auf einem mobilen Gerät geladen hat;

[0052] Fig. 7 eine schematische Ansicht einer möglichen Ausführungsform, bei der ein Benutzer von einem nicht verpixelten Bild ein Screen-Shot erstellt; und

[0053] Fig. 8 eine schematische Ansicht einer Ausführungsform, bei der ein Benutzer ein auf einem Display des mobilen Geräts dargestellten Bildes mit einem anderen mobilen Gerät dieses Bild abphotographiert.

[0054] Für gleiche oder gleich wirkende Elemente der Erfindung werden identische Bezugszeichen verwendet. Ferner werden der Übersicht halber nur Bezugszeichen in den einzelnen Figuren dargestellt, die für die Beschreibung der jeweiligen Figur erforderlich sind.

[0055] Fig. 1 zeigt eine schematische Ansicht eines mobilen Geräts **2** (Smartphone), mit dem ein Benutzer das erfindungsgemäße Anwendungsprogramm **12** aufrufen kann, um mit dem erfindungsgemäßen Anwendungsprogramm **12** alphanumerische und/oder bildliche Datensätze **10** (siehe **Fig.** 3) zu versenden. Auf einem Display **3** des mobilen Geräts **2** wird das Anwendungsprogramm **12** mit einem Logo **13** dargestellt. Das Anwendungsprogramm **12** kann über das Logo **13** aufgerufen werden.

[0056] Fig. 2 zeigt eine schematische Ansicht des mobilen Geräts **2** mit den erforderlichen Einrichtungen zur Ausführung des erfindungsgemäßen Anwendungsprogramms **12**. Das mobile Gerät **2** besitzt einen Prozessor **5**, mit dem computerlesbare Anweisungen des Anwendungsprogramms **12** ausführbar sind. Ferner ist ein nichtflüchtiges computerlesbares Speichermedium **6** vorhanden, in dem die computerlesbaren Anwendungen gespeichert sind. Über den Prozessor **5** werden die computerlesbaren Anweisungen aus dem Speichermedium **6** abgerufen. Ferner ist eine Kamera **4** des mobilen Geräts **2** mit dem Prozessor **5** kommunikativ verbunden. Der Prozessor **5** verarbeitet somit die durch die Kamera **4** aufgenommenen Bilder. Ebenso ist der Prozessor **5** mit einem drahtlosen Transceiver **9** verbunden. Ebenso ist der Prozessor **5** mit einem Eingabemittel **7** verbunden, über das ein Benutzer des mobilen Geräts **2** Anweisungen und Eingaben machen kann, die mit dem Prozessor **5** des mobilen Geräts **2** ausgeführt werden. Hinzu kommt, dass der Prozessor **5** wechselseitig mit einem Kommunikationsmittel **8** verbunden ist.

[0057] Fig. 3 zeigt eine schematische Darstellung des Ablaufs des Versendens von alphanumerischen und/oder bildlichen Datensätzen **10**. In einer Cloud **20** sind mehrere alphanumerische und/oder bildliche Datensätze **10** gespeichert. Der Benutzer eines mobilen Geräts **2** kann nun mindestens einen dieser alphanumerischen und/oder bildlichen Datensätze **10** aus der Cloud **20** abrufen und sich auf dem Display

3 des mobilen Geräts **2** anzeigen lassen. Bei der hier dargestellten Ausführungsform ist der alphanumerische und/oder bildliche Datensatz **10** ein Bild. Mit dem Anwendungsprogramm **12**, das auf dem mobilen Gerät **2** installiert ist, kann der Benutzer des mobilen Geräts **2** aus dem alphanumerischen und/oder bildlichen Datensatz **10** einen verpixelten Datensatz **11** erzeugen. Bevor dieser verpixelte Datensatz **11** versendet wird, wählt der Benutzer aus einer Kontaktliste **30** diejenigen Kontakte K1, K2, ..., KN aus, die den alphanumerischen und/oder bildlichen Datensatz **10** unverpixelt betrachten können und dürfen.

[0058] Fig. 4 zeigt eine schematische Darstellung des Ablaufs des Verfahrens, mit dem ein verpixelter Datensatz **11** versendet wird und wie dieser von einem der berechtigten Kontakte K1, K2, ..., KN nicht verpixelt betrachtet werden kann. Wie bereits in der Beschreibung zu **Fig.** 3 erwähnt, wählt ein Versender V auf seinem mobilen Gerät **2** diejenigen Kontakte K1, K2, ..., KN aus, die den von ihm versendeten verpixelten Datensatz **11** ohne die Verpixelung betrachten dürfen. In der hier dargestellten Beschreibung wählt der Versender V die Kontakte K1 und K2 aus. Von dem mobilen Gerät **2** des Versenders V gelangt die Auswahl der Kontakte K1 und K2 mit einer Benachrichtigung **15** an einen Server **40**. Ebenso wird dem Server **40** mitgeteilt, dass die Kontakte K1 und K2 eine Nachricht **16** erhalten sollen, dass von dem Versender V ein verpixelter Datensatz **11** gesendet worden ist. Der Kontakt K1 ruft nun auf seinem mobilen Gerät **21** das Anwendungsprogramm **12** (siehe **Fig.** 1) auf und wandelt den verpixelten Datensatz **11** in einen alphanumerischen und/oder bildlichen Datensatz **10** um, der nicht verpixelt ist. Mit dem Anwendungsprogramm kann der Benutzer K1 nun das Bild **10** ohne die Verpixelung betrachten. Das mobile Gerät **21** des Kontakts K1 prüft vorher über den Server **40** nach, ob dem Kontakt K1 auch die Berechtigung zusteht, einen verpixelten Datensatz **11** nicht verpixelt zu betrachten.

[0059] Dem Kontakt K2 wurde ebenfalls über eine Nachricht **16** angezeigt, dass er vom Versender V einen verpixelten Datensatz **11** empfangen hat. Der Benutzer K2 besitzt in diesem Fall auch das erforderliche Anwendungsprogramm **12**. Folglich übermittelt der Benutzer K2 an den Server **40** eine Nachricht **17**, dass er nicht berechtigt ist, den verpixelten Datensatz **11** unverpixelt zu betrachten. Für den Fall, dass ihm vom Versender V die Berechtigung erteilt wird, erhält er über den Server **40** eine Rückmeldung **18**, mit der ihm die Berechtigung erteilt wird. Über das Anwendungsprogramm **12** auf seinem mobilen Gerät $\mathbf{2}_2$ geladen hat, kann er letztendlich den verpixelten Datensatz **11** unverpixelt betrachten.

[0060] Fig. 5 zeigt eine schematische Darstellung der Situation, bei der ein Kontakt K1, K2, ..., KN das Anwendungsprogramm **12** auf seinem mobilen Gerät $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$ geladen hat. Der Kontakt K1, K2, ..., KN erhält vom Versender V einen verpixelten Datensatz **11**, auf dem auch das Logo **13** des Anwendungsprogramms dargestellt ist. Da er ein berechtigter Kontakt K1, K2, ..., KN ist, kann er über den Aufruf des Anwendungsprogramms **12** auf dem Display **3** des mobilen Geräts $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$ den verpixelten Datensatz **11** derart behandeln, dass auf dem Display **3** des mobilen Geräts $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$ das nicht verpixelte Bild **10** dargestellt wird.

[0061] In **Fig.** 6 ist die Situation dargestellt, dass ein Kontakt K1, K2, ..., KN den verpixelten Datensatz **11** empfängt, aber diesen nicht unverpixelt betrachten kann, da ihm hierzu das erforderliche Anwendungsprogramm **12** fehlt. Da auf dem verpixelten Datensatz **11** das Logo **13** des Anwendungsprogramms **12** dargestellt ist, kann der Kontakt K1, K2, ..., KN dem Versender V eine Nachricht **16** zukommen lassen und ihn darum bitten, ihm die Berechtigung für das nicht verpixelte Betrachten des verpixelten Datensatzes **11** zu erteilen. Parallel dazu kann sich der Kontakt K1, K2, ..., KN das Anwendungsprogramm **12** auf sein mobiles Gerät $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$ laden. Nachdem er vom Versender V die Berechtigung **15** erhalten hat, kann er mit dem Anwendungsprogramm den verpixelten Datensatz **11** bereinigen und das Bild **10** betrachten.

[0062] Die gesamte Kommunikation in den **Fig.** 5 und **Fig.** 6 mit dem Server **40** (siehe **Fig.** 4) und die Berechnung und Ermittlung der Berechtigungen geschieht auf dem Server **40** in Echtzeit. Ein Benutzer des Anwendungsprogramms **12** merkt somit keine Zeitverzögerung bei dem Betrachten, bzw. Bereinigen der verpixelten Datensätze **11**.

[0063] Fig. 7 zeigt eine Situation, bei der ein berechtigter Kontakt K1, K2, ..., KN von dem auf dem Display **3** dargestellten Bild **10** einen Screenshot **22** anfertigt, um diesen Screenshot **22** ungehindert in anderen sozialen Netzwerken zu verteilen. Um dies zu verhindern, kann z. B. wie in **Fig.** 7 dargestellt, über den angefertigten Screenshot **22** eine schwarze Fläche **24** gelegt werden. Es ist für einen Fachmann selbstverständlich, dass hierfür jegliche Art der Unkenntlichmachung des durch einen Screenshot **22** angefertigten Bildes **10** möglich ist. Ebenso ist es denkbar, dass auf dem Bild **10** die Kennung **26** des berechtigten Benutzers K1, K2, ..., KN eingeblendet wird. Über diese Kennung **26** kann auch immer nachvollzogen werden, von wem der Screenshot **22** angefertigt worden ist, der nun ohne eine Verpixelung in den sozialen Netzwerken kursiert.

[0064] Fig. 8 zeigt eine andere Möglichkeit, bei dem mit einem zusätzlichen mobilen Gerät $\mathbf{2}_Z$ das auf dem Display **3** des mobilen Geräts $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$ des Empfängers abphotographiert wird. Um dies nachzuvollziehen, dass das nicht verpixelte Bild **10** mit einem zusätzlichen mobilen Gerät $\mathbf{2}_Z$ abphotographiert wor-

den ist, wird in dem ursprünglichen, auf dem mobilen Gerät **2**$_1$, **2**$_2$, ..., **2**$_N$ des Empfängers eine Kennung **26** eingeblendet. Dadurch kann immer erkannt werden, dass ein Bild von einem zusätzlichen mobilen Gerät **2**$_Z$ abphotographiert worden ist. Somit lässt sich immer der Kontakt K1, K2, ..., KN auffinden, der das Bild abphotographiert hat. Gemäß den AGB's des Anwendungsprogramms **12** kann somit den Benutzer K1, K2, ..., KN die Berechtigung zur Verwendung des Anwendungsprogramms **12** entzogen werden.

[0065] Ebenso hat die Erfindung den Vorteil, dass das erfindungsgemäße Anwendungsprogramm **12** mit einem Code oder einem Muster geschützt ist. Somit ist auch für den Fall eines Verlusts des mobilen Geräts **2**$_1$, **2**$_2$, ..., **2**$_N$ sichergestellt, dass nur der berechtigte Benutzer des mobilen Geräts **2**$_1$, **2**$_2$, ..., **2**$_N$ das Anwendungsprogramm aufrufen kann und somit die berechtigten Bilder nicht verpixelt betrachten kann. Ebenso ist es von Vorteil, dass die in dem Anwendungsprogramm zugewiesenen Album vorhandenen Bilder jederzeit wieder aufgerufen werden können, da es, wie bereits erwähnt, von Vorteil ist, die dem Anwendungsprogramm **12** zugewiesenen Bilder bzw. alphanumerischen und/oder bildlichen Datensätze **10** in einer Cloud **20** zu speichern.

Bezugszeichenliste

2	mobiles Gerät des Versenders
2$_1$, 2$_2$, ..., 2$_N$	mobiles Gerät des Empfängers
2$_Z$	zusätzliches mobiles Gerät
3	Display
4	Kamera
5	Prozessor
6	Speichermedium
7	Eingabemittel
8	Kommunikationsmittel
9	Drahtloser Transceiver
10	alphanumerischer und/oder bildlicher Datensatz; Bild
11	verpixelter Datensatz
12	Anwendungsprogramm
13	Logo
15	Berechtigung
16	Nachricht
17	Nachricht nicht berechtigter Kontakt
18	Rückmeldung
20	Cloud
22	Screenshot
24	schwarze Fläche
26	Kennung
30	Kontaktliste
40	Server
K1, K2, ..., KN	Kontakt
V	Versender

Patentansprüche

1. Verfahren zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit (**2**) eines Versenders (V) und mindestens einer Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) eines ausgewählten Kontakts (K1, K2, ..., KN) gekennzeichnet durch die folgenden Schritte:
• dass ein Anwendungsprogramm gestartet wird;
• dass von einem Versender (V) ein alphanumerischer und/oder bildlicher Datensatz (**10**) ausgewählt wird, der vom Versender (V) an mindestens einen aus einer Kontaktliste (**30**) ausgewählten Kontakt (K1, K2, ..., KN) versendet wird;
• dass dem mindestens einen ausgewählten Kontakt (K1, K2, ..., KN) eine Berechtigung (**15**) vom Versender (V) zugewiesen wird, wobei die Datenverarbeitungseinheit (**2**) des Versenders (V) mit einem Server (**40**) kommuniziert, so dass die Berechtigung (**15**) auf dem Server (**40**) gespeichert wird;
• dass der ausgewählte alphanumerische und/oder bildliche Datensatz (**10**) vor dem Versenden an den mindestens einen ausgewählten Kontakt (K1, K2, ..., KN) verpixelt und als verpixelter Datensatz (**11**) an eine Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) des mindestens einen Kontakts (K1, K2, ..., KN) übermittelt wird;
• dass die Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) des mindestens einen ausgewählten Kontakts (K1, K2, ..., KN) mit den Server (**40**) kommuniziert und die Berechtigung (**15**) abfragt;
• dass bei Berechtigung (**15**) des Kontakts die Verpixelung des vom Versender (V) versendeten und verpixelten Datensatzes (**11**) entfernt wird;
• dass falls ein von einem berechtigten Kontakt (K1, K2, ..., KN) angefertigter Screenshot (**22**) des empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatzes (**10**) zumindest teilweise unkenntlich gemacht wird und/oder mit einer Kennung (**26**) des berechtigten Kontakts (K1, K2, ..., KN) versehen wird; und
• dass falls ein von der Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) eines berechtigten Kontakts (K1, K2, ..., KN) ein alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz (**10**) mit einer weiteren Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) abfotographiert wird, der alphanumerische und/oder bildliche und nicht verpixelte Datensatz mit einer Kennung (**26**) versehen wird.

2. Verfahren nach Anspruch 1, wobei der versendete und verpixelte Datensatz (**11**) mit einem Logo (**13**) eines Anwendungsprogramms (**12**) versehen wird, wobei das Logo (**13**) einem berechtigten Kontakt (K1, K2, ..., KN) anzeigt, dass zum nicht verpixel-

ten Betrachten des empfangenen verpixelten Datensatzes (**11**) zuerst das Anwendungsprogramm (**12**) auf die Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) geladen werden muss.

3. Verfahren nach Anspruch 2, wobei ein nicht berechtigter Kontakt (K1, K2, ..., KN) eine Nachricht (**17**) an den Versender (V) sendet, um eine Berechtigung für das nicht verpixelte Betrachten der empfangenen alphanumerischen (**15**) und/oder bildlichen Datensatzes (**10**) zu erhalten und dass diese dem Server (**40**) mitgeteilt wird.

4. Verfahren nach einem der vorangehenden Ansprüche, wobei die von dem mindestens einen berechtigten Kontakt (K1, K2, ..., KN) empfangenen alphanumerischen und/oder bildlichen Datensätze (**10**) in einem dem Anwendungsprogramm (**12**) zugewiesenen Album gespeichert werden, wobei ein Versenden des empfangenen alphanumerischen und/oder bildlichen Datensatzes (**10**) verpixelt erfolgt und keine weiteren Berechtigung (**15**) zugewiesen werden als diejenigen, die bereits von ursprünglichen Versender (V) vergeben worden sind.

5. Verfahren nach einem der vorangehenden Ansprüche, wobei die Datenverarbeitungseinheiten (**2**, **2**$_1$, **2**$_2$, ..., **2**$_N$) als mobile Geräte ausgebildet sind.

6. Verfahren nach Anspruch 5, wobei das Anwendungsprogramm (**12**) der mobilen Geräte (**2**$_1$, **2**$_2$, ..., **2**$_N$) mit einem Code oder einem Muster geschützt wird, so dass für den Fall eines Verlusts des mobilen Geräts (**2**$_1$, **2**$_2$, ..., **2**$_N$) sichergestellt ist, dass nur der berechtigte Benutzer des mobilen Geräts (**2**$_1$, **2**$_2$, ..., **2**$_N$) das Anwendungsprogramm aufrufen kann und somit die berechtigten Bilder nicht verpixelt betrachten kann.

7. Ein nicht flüchtiges computerlesbares Speichermedium (**6**), das computerlesbare Anweisungen eines Anwendungsprogramms (**12**) umfasst, die auf dem Speichermedium (**6**) gespeichert sind, wobei die computerlesbare Anweisungen auf mindestens einen Prozessor (**5**) mindestens einer Datenverarbeitungseinheit (**2**) eines Versenders (V) und auf mindestens einen Prozessor (**5**) einer Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) mindestens eines Kontakts (K1, K2, ..., KN) ausführbar sind, um eine computergestützte, sichere und kontrollierbare Kommunikation mit mindestens einer Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) mindestens eines Kontakts (K1, K2, ..., KN) herzustellen, **dadurch gekennzeichnet,** dass
• ein vom Versender (V) ausgewählter alphanumerischer und/oder bildlicher Datensatz (**10**) vor dem Versenden an den mindestens einen ausgewählten Kontakt (K1, K2, ..., KN) als ein verpixelter Datensatz (**11**) auf einem Display (**3**) der Datenverarbeitungseinheit (**2**) des Versenders (V) dargestellt wird,
• der Versender (V) mindestens einen Kontakt (K1, K2, ..., KN) aus einer Kontaktliste (**30**) ausgewählt, an den der verpixelte Datensatz (**11**) versendet wird;
• eine Berechtigung (**15**) vom Versender (V) an einen Server (**40**) übermittelt und dort gespeichert wird, die anzeigt, dass der mindestens eine ausgewählte Kontakt (K1, K2, ..., KN) den alphanumerischen und/oder bildlichen Datensatz (**10**) nicht verpixelt betrachten kann;
• nach Empfangen einer Nachricht (**16**) des Versenders (V), dass ein verpixelter Datensatz (**11**) gesendet wurde, die Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) des mindestens einen ausgewählten Kontakts (K1, K2, ..., KN) mit den Server (**40**) kommuniziert und die Berechtigung (**15**) abfragt;
• dass bei auf dem Server (**40**) vorliegenden Berechtigung (**15**) des Kontakts (K1, K2, ..., KN) die Verpixelung des vom Versender (V) versendeten verpixelten Datensatzes (**11**) entfernt wird;
• dass falls ein Screenshot (**22**) von empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatz (**10**) zumindest teilweise unkenntlich gemacht wird und/oder mit einer Kennung (**26**) des berechtigten Kontakts (K1, K2, ..., KN) versehen wird; und
• dass falls ein von der Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) eines berechtigten Kontakts (K1, K2, ..., KN) ein alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz (**10**) mit einer weiteren Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) abfotographiert wird, der alphanumerische und/oder bildliche und nicht verpixelte Datensatz mit einer Kennung (**26**) versehen wird..

8. Nicht flüchtiges computerlesbares Speichermedium (**6**) mit den computerlesbare Anweisungen nach Anspruch 7, wobei der versendete und verpixelte Datensatz (**11**) mit einem Logo (**13**) des aus den computerlesbare Anweisungen bestehenden Anwendungsprogramms (**12**) versehen wird, wobei das Logo (**13**) des Anwendungsprogramms (**12**) einem berechtigten Kontakt (K1, K2, ..., KN) anzeigt, dass zum nicht verpixelten Betrachten des empfangenen verpixelten Datensatzes (**11**) zuerst das Anwendungsprogramm (**12**) auf die Datenverarbeitungseinheit (**2**$_1$, **2**$_2$, ..., **2**$_N$) geladen werden muss.

9. Nicht flüchtiges computerlesbares Speichermedium (**6**) mit den computerlesbaren Anweisungen nach Anspruch 7, wobei von einem nicht berechtigten Kontakt (K1, K2, ..., KN) eine Nachricht (**17**) für den Versender (V) generiert wird, um eine Berechtigung für das nicht verpixelte Betrachten des empfangenen alphanumerischen und/oder bildlichen und verpixelten Datensatzes (**11**) zu erhalten und wobei von der Datenverarbeitungseinheit (**2**) des Versenders (V) an den Server (**40**) die Berechtigung (**15**) mitgeteilt wird.

10. Nicht flüchtiges computerlesbares Speichermedium (**6**) mit den computerlesbaren Anweisungen

nach Anspruch 7, wobei die Datenverarbeitungseinheiten (**2**, $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) als mobile Geräte ausgebildet sind.

11. Nicht flüchtiges computerlesbares Speichermedium (**6**) mit den computerlesbaren Anweisungen nach Anspruch 10, wobei das Anwendungsprogramm (**12**) der mobilen Geräte ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) mit einem Code oder einem Muster geschützt wird, so dass für den Fall eines Verlusts des mobilen Geräts ($\mathbf{2}_1$, $\mathbf{2}_1$, ..., $\mathbf{2}_N$) sichergestellt ist, dass nur der berechtigte Benutzer des mobilen Geräts ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) das Anwendungsprogramm aufrufen kann und somit die berechtigten Bilder nicht verpixelt betrachten kann.

12. System zur computergestützten, sicheren und kontrollierten Kommunikation zwischen einer Datenverarbeitungseinheit (**2**) als Versender (V) und mindestens einer weiteren Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) als Empfänger umfasst:
• einen Server (**40**), mit dem die Datenverarbeitungseinheit (**2**) des Versenders (V) und die mindestens eine weitere Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$), kommunikativ verbunden sind;
• einen Prozessor (**4**) der Datenverarbeitungseinheit (**2**) des Versenders (V), auf dem ein Anwendungsprogramm (**12**) ausführbar ist, das aus einem alphanumerischen und/oder bildlichen Datensatz (**10**) einen verpixelten Datensatz (**11**) erstellt;
• ein Eingabemittel (**7**) zum auswählen mindestens eines Kontakts (K1, K2, ..., KN), an den der verpixelten Datensatz (**11**) sendbar ist und der zum Betrachten des alphanumerischen und/oder bildlichen Datensatz (**10**) ohne eine Verpixelung berechtigt ist, wobei die Berechtigung von der Datenverarbeitungseinheit (**2**) des Versenders (V) auf dem Server (**40**) hinterlegt ist;
• ein Prozessor (**4**) der mindestens einen weiteren Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$), auf dem ebenfalls das Anwendungsprogramm (**12**) ausführbar ist, um aus dem verpixelten Datensatz (**11**) den alphanumerischen und/oder bildlichen Datensatz (**10**) wieder herzustellen, wobei vor der Ausführung des Anwendungsprogramms (**12**) über die weitere Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) des mindestens einen Kontakts (K1, K2, ..., KN) die Berechtigung vom Server abrufbar ist;
• dass das Anwendungsprogramm (**12**) im der Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) derart gestaltet ist, dass falls bei einem Screenshot (**22**) des empfangenen alphanumerischen und/oder bildlichen und nicht verpixelten Datensatzes (**10**) der Screenshot (**22**) zumindest teilweise unkenntlich ist und/oder eine Kennung (**26**) der Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) trägt, mit dem der Screenshot (**22**) angefertigt wurde; und
• dass falls ein von der Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) eines berechtigten Kontakts (K1, K2, ..., KN) ein alphanumerischer und/oder bildlicher und nicht verpixelter Datensatz (**10**) mit einer weiteren Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) abfotografiert wird, der alphanumerische und/oder bildliche und nicht verpixelte Datensatz mit einer Kennung (**26**) versehen ist.

13. System nach Anspruch 12, wobei ein Logo (**13**) des Anwendungsprogramms (**12**) auf dem verpixelten Datensatz (**11**) dargestellt ist, und eine Schaltfläche darstellt, mit der das Anwendungsprogramm (**12**) auf die mindestens eine Datenverarbeitungseinheit ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) ladbar ist.

14. System Anspruch 12, wobei die Datenverarbeitungseinheiten (**2**, $\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) als mobile Geräte ausgebildet sind und das Anwendungsprogramm (**12**) der mobilen Geräte ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) mit einem Code oder einem Muster geschützt wird, so dass für den Fall eines Verlusts des mobilen Geräts ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) sichergestellt ist, dass nur der berechtigte Benutzer des mobilen Geräts ($\mathbf{2}_1$, $\mathbf{2}_2$, ..., $\mathbf{2}_N$) das Anwendungsprogramm aufrufen kann und somit die berechtigten Bilder nicht verpixelt betrachten kann.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

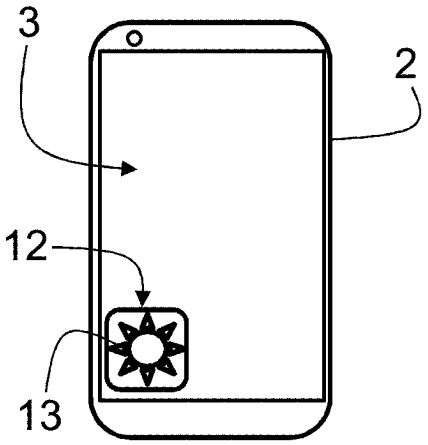


Fig. 1

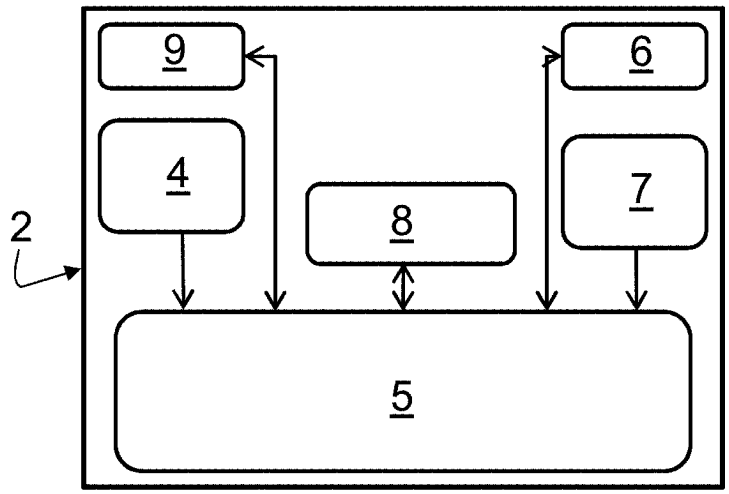


Fig. 2

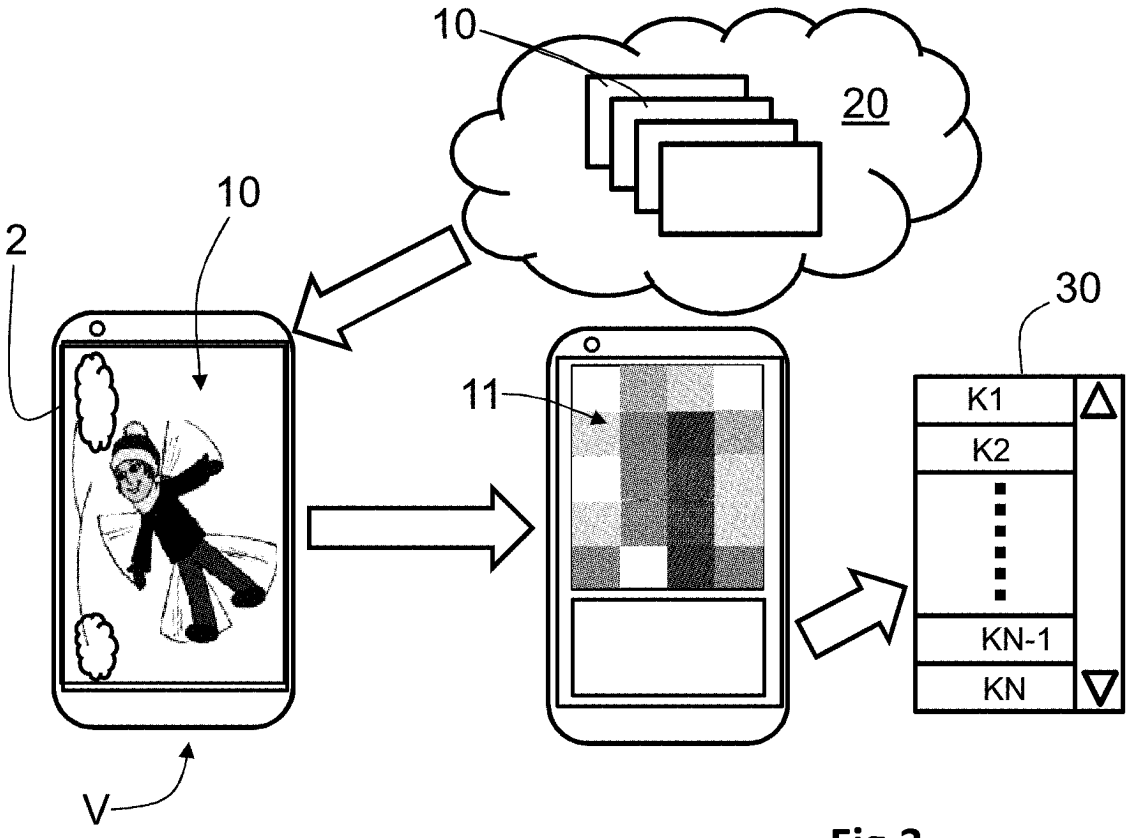


Fig.3

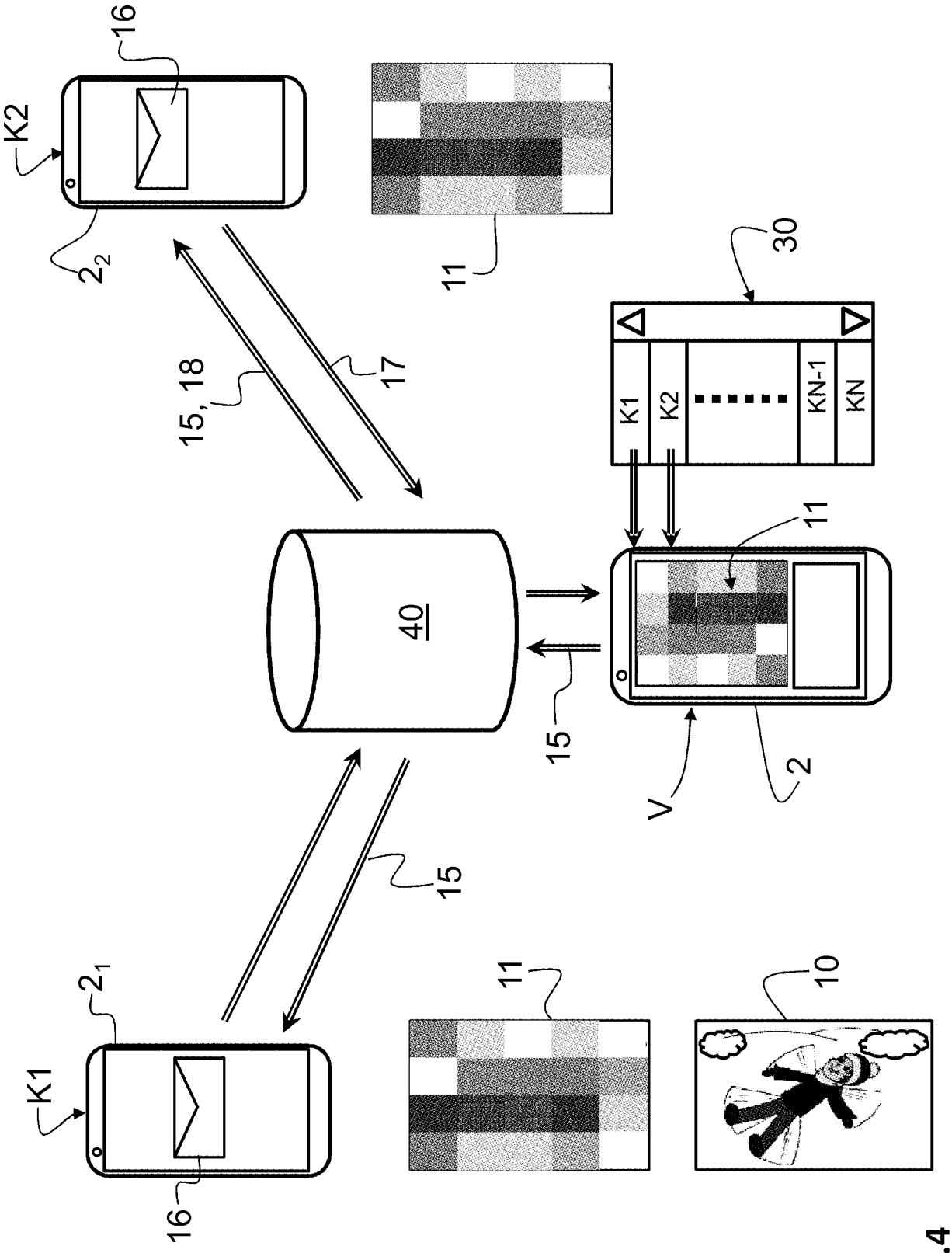


Fig.4

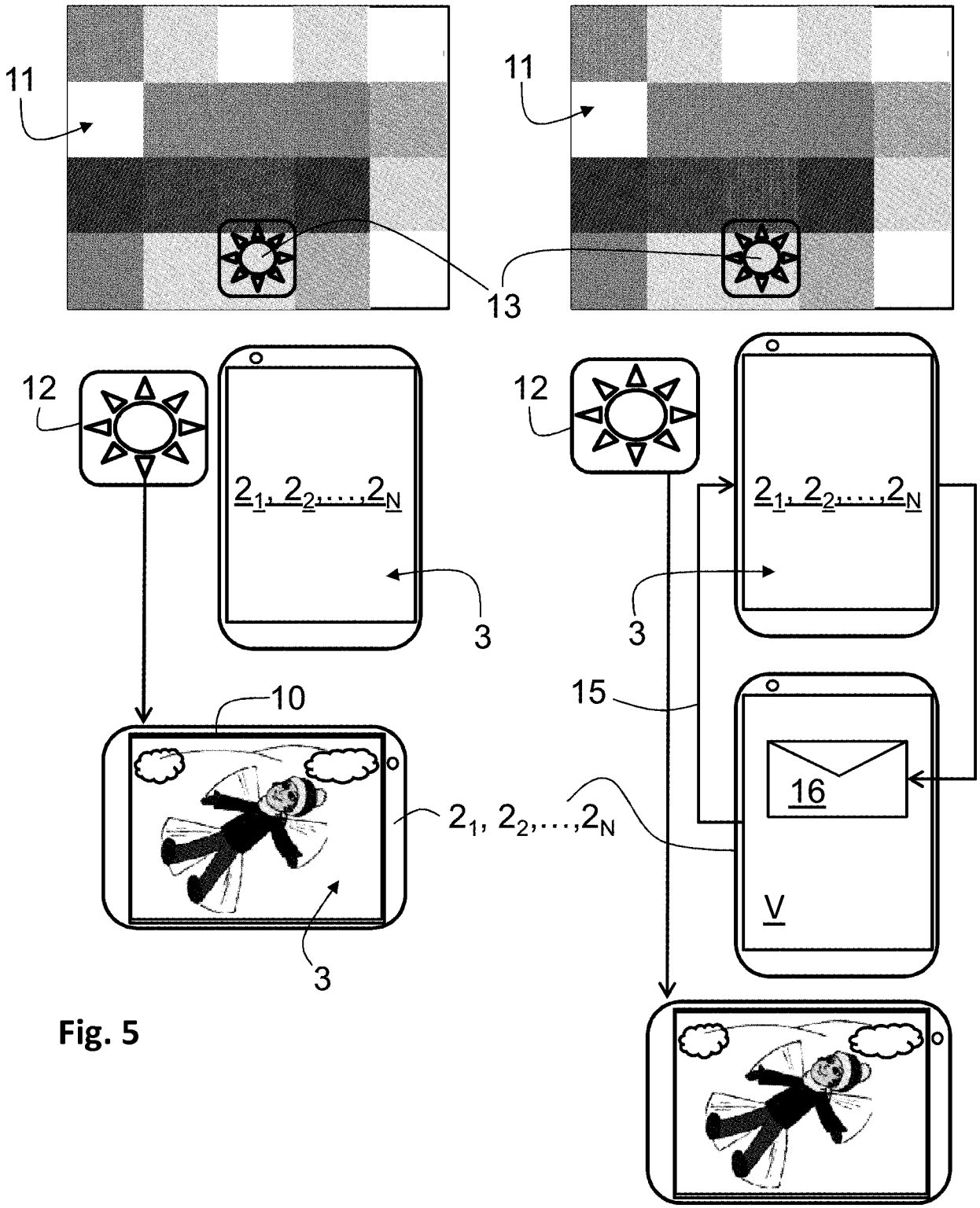

11
11
13
12
12
$2_1, 2_2, \ldots, 2_N$
$2_1, 2_2, \ldots, 2_N$
3
3
10
15
16
$2_1, 2_2, \ldots, 2_N$
V
3

Fig. 5

Fig.6

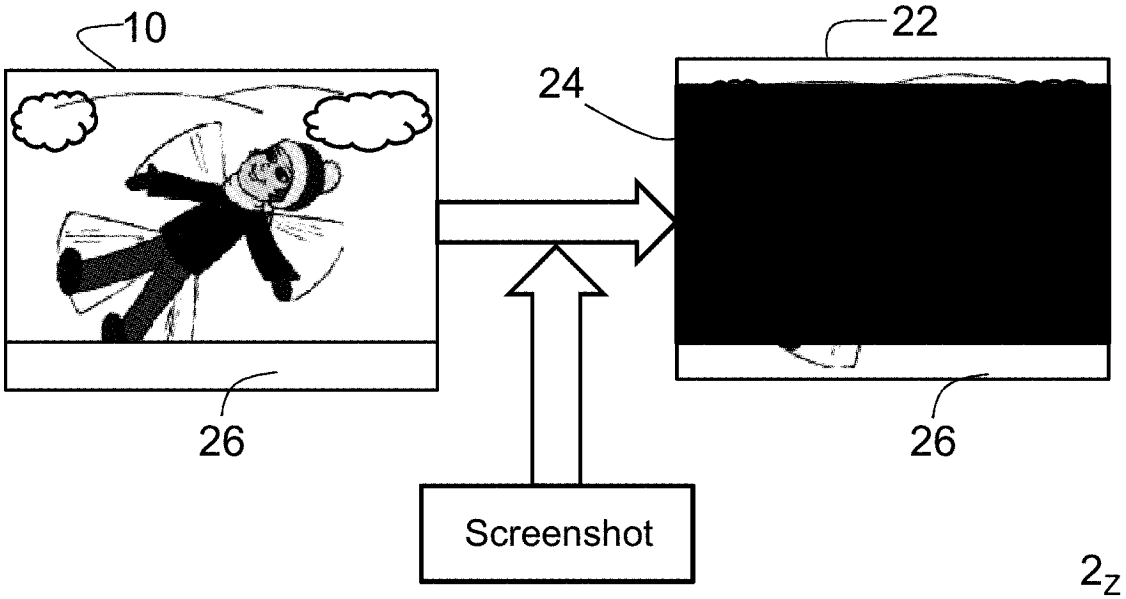

10
22
24
26
26
Screenshot
2z

Fig.7

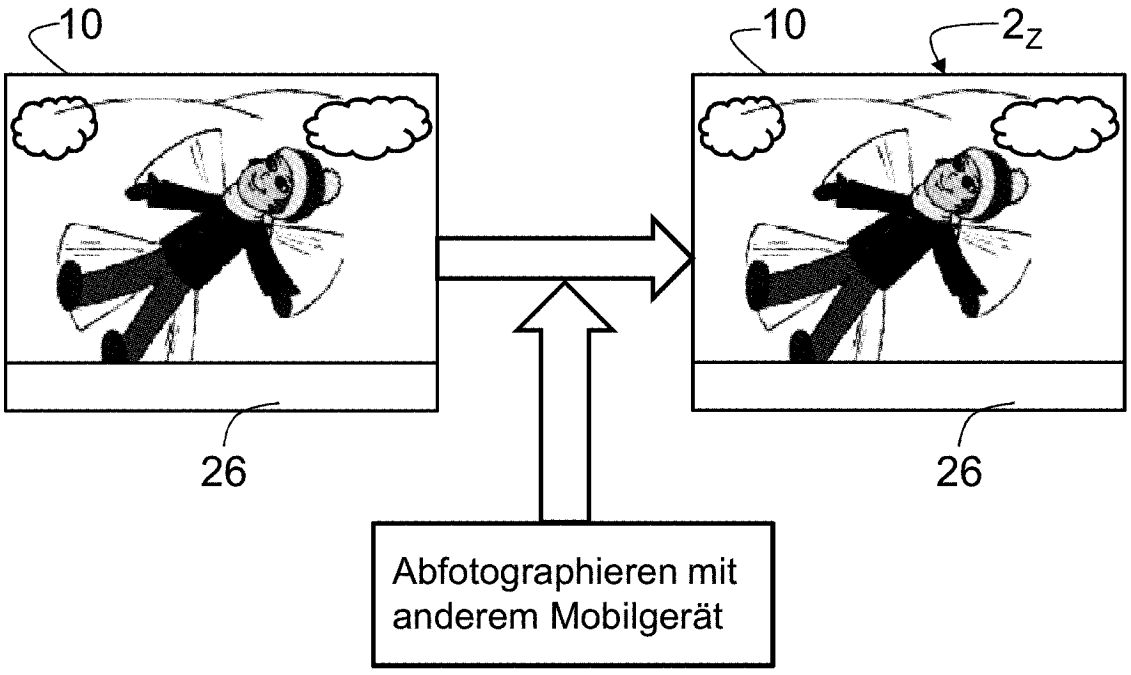

10
10
2z
26
26
Abfotographieren mit anderem Mobilgerät

Fig.8