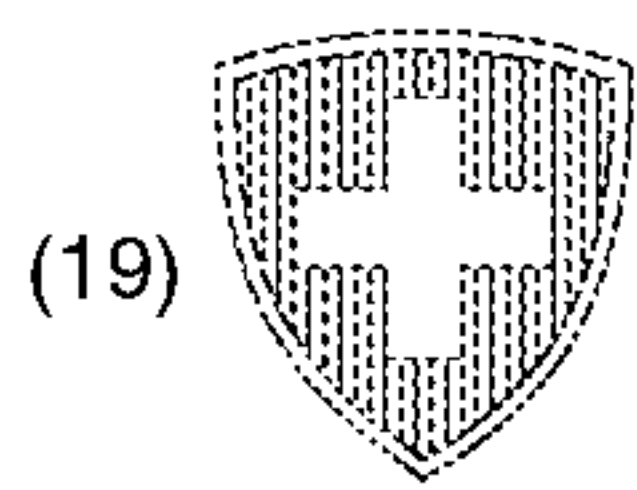




SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH** **716 052 A1**

(51) Int. Cl.: **G06K 9/00** (2006.01)

Patentanmeldung für die Schweiz und Liechtenstein

Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) **PATENTANMELDUNG**

(21) Anmeldenummer: 00483/19

(22) Anmeldedatum: 10.04.2019

(43) Anmeldung veröffentlicht: 15.10.2020

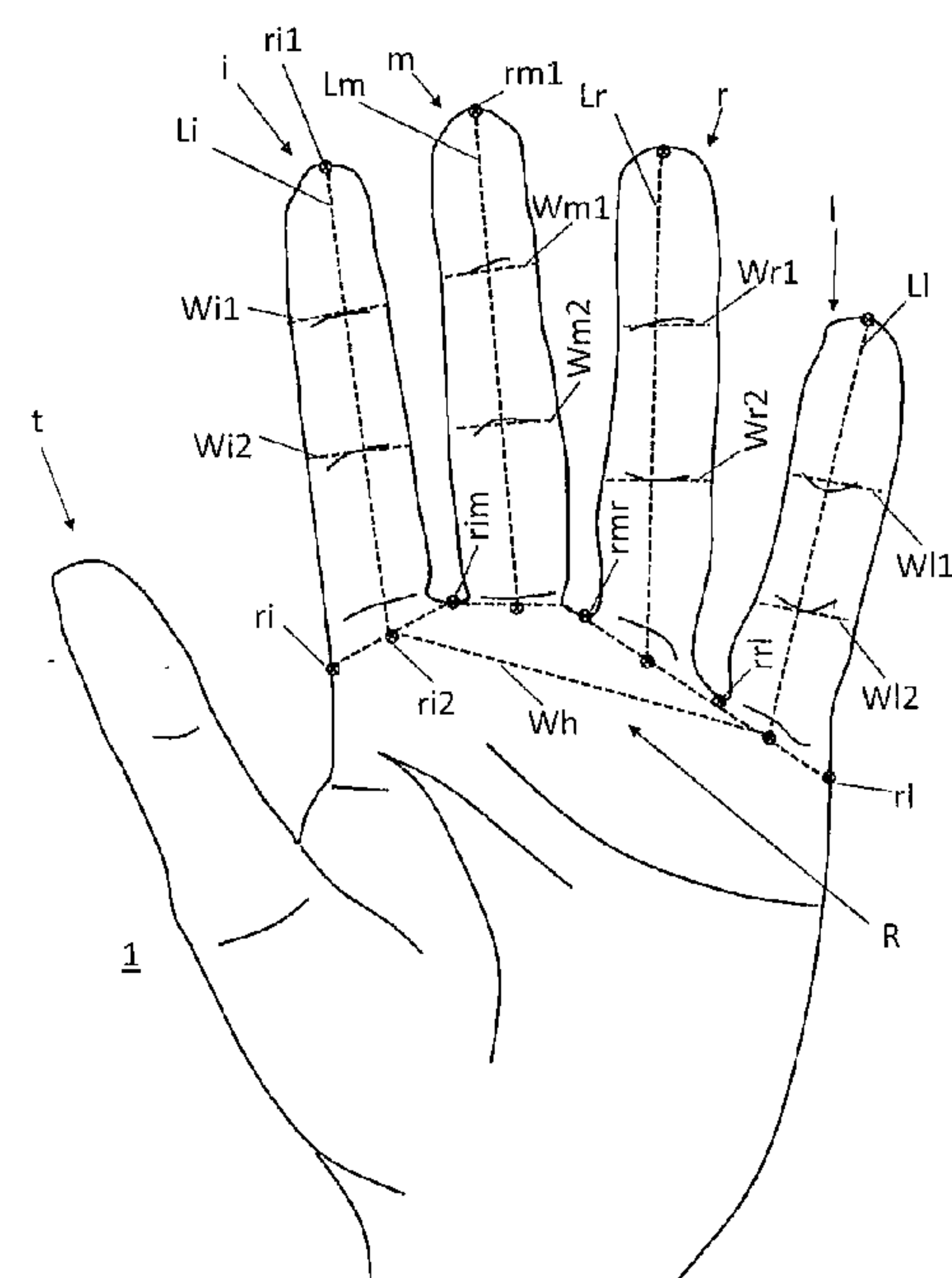
(71) Anmelder:
Smart Secure ID AG, Neuhofstrasse 5A
6340 Baar (CH)

(72) Erfinder:
Arnold Herp, 91096 Moehrendorf (DE)
Johan Bergqvist, 6300 Zug (CH)

(74) Vertreter:
Schneider Feldmann AG Patent- und Markenanwälte,
Beethovenstrasse 49 Postfach
8027 Zürich (CH)

(54) **Biometrische Authentifizierungsvorrichtung und biometrisches Authentifizierungsverfahren zur Authentifizierung einer Person mit reduzierter Rechenkomplexität.**

(57) Eine biometrische Authentifizierungsvorrichtung zum Authentifizieren einer Person durch Vergleich biometrischer Merkmale eines Körperteils der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen einer Vielzahl registrierter Personen ist konfiguriert zum: Erfassen von Bilddaten des Körperteils der Person; Bestimmen mindestens einer charakteristischen geometrischen Körperteil-Eigenschaft (Wh) des Körperteils der Person und biometrischer Merkmale des Körperteils der Person aus den erfassten Bilddaten; Beschränken des Vergleichs der biometrischen Merkmale des Körperteils der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Wh) der Person aufweisen.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Offenbarung bezieht sich auf ein biometrisches Authentifizierungsvorrichtung und ein biometrisches Authentifizierungsverfahren zur Authentifizierung einer Person. Insbesondere bezieht sich die vorliegende Offenbarung auf eine biometrische Authentifizierungsvorrichtung und ein biometrisches Authentifizierungsverfahren zur Authentifizierung einer Person mit reduzierter Rechenkomplexität.

ALLGEMEINER STAND DER TECHNIK

[0002] Biometrische Authentifizierungsvorrichtungen werden in großem Umfang für die Authentifizierung von Personen verwendet, z.B. im Zusammenhang mit der Zugangskontrolle zu Ressourcen wie zum Beispiel Gebäuden, Räumen, Computern, Smartphones, elektronischen Bankkonten, Wahlsystemen, Schul- oder Universitätsprüfungsunterlagen, Grenzen, Firmenregistern usw.

[0003] In einigen Ausführungsformen sind biometrische Authentifizierungsvorrichtungen so konfiguriert, dass sie Bilddaten eines Körperteils einer Person, z.B. einer Hand der Person, erfassen und aus den erfassten Bilddaten individuelle und typische biometrische Merkmale bestimmen. Erfasste Bilddaten der Hand oder eines Körperteils der Person können sich auf Bilddaten beziehen, die mit einem Sensor für Nahinfrarotlicht (z.B. 700 nm bis 900 nm) erfasst wurden, auf Bilddaten, die mit einem Sensor für sichtbares Licht (z.B. 400 nm bis 600 nm) erfasst wurden, oder einer Kombination davon. Biometrische Merkmale die aus Bilddaten bestimmt wurden können sich auf Venenmuster, Handabdrücke, Lebenslinien usw. der Hand beziehen. Im Nahinfrarotlichtspektrum erfasste Bilddaten ermöglichen die Bestimmung von Merkmalen, die sich auf Venenmuster der Hand beziehen. Im sichtbaren Lichtspektrum erfasste Bilddaten ermöglichen die Bestimmung von Merkmalen, die sich auf Handabdrücke und Lebenslinien der Hand beziehen.

[0004] Die Authentifizierung von Personen basiert auf vorgeschichteten biometrischen Merkmalen, die unter der Kontrolle einer dazu berechtigten und vertrauenswürdigen Instanz registriert wurden. Diese Instanz überprüft die Identität einer Person anhand eines Ausweises, wie z.B. eines Reisepasses. Entsprechende Bilddaten der Hand der Person werden erfasst und aus den erfassten Bilddaten werden biometrische Merkmale der Hand oder eines Körperteils der Person bestimmt. Die bestimmten biometrischen Merkmale werden in einer Datenbank als vorgeschichtete biometrische Merkmale gespeichert. In einigen Ausführungsformen können die vorgeschichteten biometrischen Merkmale die erfassten Bilddaten teilweise oder vollständig enthalten. Die bestimmten biometrischen Merkmale der Hand oder eines Körperteils, die erfassten Bilddaten der Hand oder eine Kombination davon können sich auf Venenmuster, Handabdrücke, Lebenslinien usw. beziehen.

[0005] Später, wenn die Authentifizierung einer Person erforderlich ist, erfasst eine biometrische Authentifizierungsvorrichtung Bilddaten der Hand oder eines Körperteils der Person. Biometrische Merkmale der Hand oder eines Körperteils der Person werden bestimmt und mit vorgeschichteten biometrischen Merkmalen und/oder vorgeschichteten Bilddaten verglichen. Die Authentifizierung wird für die Person genehmigt, wenn eine Übereinstimmung innerhalb der vorgeschichteten biometrischen Merkmale gefunden wird, andernfalls wird die Authentifizierung abgelehnt.

[0006] Solange sich die vorgeschichteten biometrischen Merkmale nur auf wenige Personen beziehen, z.B. auf weniger als einige Dutzend Personen, kann der Vergleich der biometrischen Merkmale mit einem „Brute-force“-Verfahren eine ausreichend schnelle Reaktionszeit von z.B. 1 Sekunde oder weniger ergeben. Wenn sich die vorgeschichteten biometrischen Merkmale z.B. auf 1 000 Personen oder mehr beziehen, ist die Rechenkomplexität stark erhöht und der Vergleich der biometrischen Merkmale erfordert eine ausreichend hohe Rechenleistung, um zum Beispiel Antwortzeiten von 1 Sekunde oder weniger zu erreichen. Eine hohe Rechenleistung führt jedoch zu einem hohen Stromverbrauch, da ausreichend schnelle Computer mit zum Beispiel Parallelverarbeitungsfähigkeiten erforderlich sind. Dementsprechend sind komplexe und teure Anlagen erforderlich. Aus diesen Gründen ist der breite Einsatz der Authentifizierung von Personen auf der Grundlage der biometrischen Merkmale einer Hand oder eines Körperteils derzeit beschränkt.

[0007] Im Stand der Technik ist bekannt, dass es die Suche nach einem Objekt in einer Datenbank beschleunigt, wenn jedem Objekt ein eindeutiger Schlüssel zugewiesen wird. Beispielsweise ist es gängige Praxis, dass persönliche Karten von Personen, wie Personalausweise oder Kreditkarten, jeweils einen eindeutigen Schlüssel aufweisen. Eine Kartenlesevorrichtung, die den Zugang zu einer bestimmten Ressource kontrolliert, wie z.B. den Eingang eines Gebäudes oder den Kontostand einer Kreditkarte, liest den Schlüssel der persönlichen Karte einer bestimmten Person und gewährt der Person Zugang zu der Ressource, wenn eine Übereinstimmung des Schlüssels in einer vorgeschichteten Datenbank gefunden werden kann. Die Suche nach einem eindeutigen Schlüssel in einer vorgeschichteten Datenbank ist präzise und schnell.

[0008] Es ist nicht möglich, biometrischen Merkmalen der Hand oder eines Körperteils einer Person einen eindeutigen Schlüssel zuzuweisen, da die Übereinstimmung biometrischer Merkmale der Hand oder eines Körperteils der Person auf einem Ähnlichkeitsmaß zwischen den biometrischen Merkmalen, die mit einem biometrischen Authentifizierungsvorrichtung bestimmt wurden, und den vorgeschichteten biometrischen Merkmalen basieren muss. Zum Beispiel muss die Differenz zwischen zwei n-dimensionalen Merkmalsvektoren bestimmt werden, und diese Differenz muss mit einem ausreichend kleinen Schwellenwert verglichen werden. Da biometrische Merkmale der Hand oder eines Körperteils einer Person nicht einem eindeutigen Schlüssel zugeordnet werden können, können die nach dem Stand der Technik bekannten Techniken nicht zur Suche eines eindeutigen Schlüssels in einer vorgeschichteten Datenbank verwendet werden.

[0009] Das Dokument „On Hierarchical Palmprint Coding With Multiple Features for Personal Identification in Large Databases (You et al.), IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 2, FEBRUARY 2004“ schlägt ein hierarchisches Multifeature-Codierungsschema vor, um das Coarse-to-fine-Matching für eine effiziente und effektive Überprüfung des Handabdrucks in einer großen Datenbank zu erleichtern. Es werden globale geometriebasierte Schlüsselpunkt-Abstände (Level-1-Merkmal), globale Texturenergie (Level-2-Merkmal), unscharfe „interessierende“ Linie (Level-3-Merkmal) und lokale gerichtete Texturenergie (Level-4-Merkmal) definiert.

KURZDARSTELLUNG DER ERFINDUNG

[0010] Es ist eine Aufgabe der Erfindung, eine biometrische Authentifizierungsvorrichtung und ein biometrisches Authentifizierungsverfahren bereitzustellen, die mindestens einige der Nachteile des Standes der Technik nicht aufweisen. Insbesondere ist es eine Aufgabe der Erfindung, eine biometrische Authentifizierungsvorrichtung und ein biometrisches Authentifizierungsverfahren mit reduzierter Rechenkomplexität bereitzustellen. Insbesondere ist es eine Aufgabe der Erfindung, eine biometrische Authentifizierungsvorrichtung und ein biometrisches Authentifizierungsverfahren bereitzustellen, die die Authentifizierung von Personen unter Verwendung von aktuellen Standard-Computervorrichtungen ermöglichen.

[0011] Mindestens eine Aufgabe der Erfindung wird durch die biometrische Authentifizierungsvorrichtung und das biometrische Authentifizierungsverfahren erreicht, die in den beigefügten unabhängigen Ansprüchen definiert sind.

[0012] Die abhängigen Ansprüche legen weitere Ausführungsformen der Erfindung dar.

[0013] Mindestens eine Aufgabe der Erfindung wird durch eine biometrische Authentifizierungsvorrichtung zum Authentifizieren einer Person durch Vergleich biometrischer Merkmale eines Körperteils der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen einer Vielzahl von registrierten Personen erreicht, wobei die biometrische Authentifizierungsvorrichtung konfiguriert ist zum: Erfassen von Bilddaten des Körperteils der Person; Bestimmen aus den erfassten Bilddaten mindestens einer charakteristischen geometrischen Körperteil-Eigenschaft des Körperteils der Person und biometrischer Merkmale des Körperteils der Person; Beschränken des Vergleichs der biometrischen Merkmale des Körperteils der Person auf vorgespeicherte biometrische Merkmale von Körperteilen der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft der Person aufweisen. Da der Vergleich biometrischer Merkmale auf vorgespeicherte biometrische Merkmale beschränkt wird, die einen vordefinierten Ähnlichkeitsgrad der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft aufweisen, ist der Vergleich auf eine Teilmenge vorgespeicherter biometrischer Merkmale beschränkt und die Rechenkomplexität daher reduziert.

[0014] In einer Ausführungsform ist das biometrische Authentifizierungsvorrichtung ferner so konfiguriert, dass sie Bilddaten mit mindestens einem Sensor für sichtbares Licht, einem Sensor für Nahinfrarotlicht, einem kombinierten Sensor für sichtbares Licht und Nahinfrarotlicht und/oder einer Laufzeitkamera erfasst. Der Sensor für sichtbares Licht, der Sensor für Nahinfrarotlicht und/oder die Laufzeitkamera können in der biometrischen Authentifizierungsvorrichtung enthalten sein. Biometrische Merkmale können unter Verwendung von Bilddaten, die mit dem Sensor für sichtbares Licht erfasst wurden, und/oder Bilddaten, die mit dem Sensor für Nahinfrarotlicht erfasst wurden, bestimmt werden. Die mindestens eine charakteristische geometrische Körperteil-Eigenschaft kann mit Bilddaten bestimmt werden, die mit der Laufzeitkamera aufgenommen wurden. Die Laufzeitkamera ermöglicht die Bestimmung der charakteristischen geometrischen Körperteil-Eigenschaft mit hoher Genauigkeit, und vorgespeicherte biometrische Merkmale mit dem vordefinierten Ähnlichkeitsgrad der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft können präzise bestimmt werden, und der Rechenaufwand dadurch weiter reduziert werden.

[0015] In einer Ausführungsform ist die biometrische Authentifizierungsvorrichtung so konfiguriert, dass sie eine Benutzerführung auf der Grundlage der mit der Laufzeitkamera aufgenommenen Bilddaten bereitstellt.

[0016] In einer Ausführungsform bezieht sich die Benutzerführung auf das Bewegen des Körperteils in eine vordefinierte Haltung, insbesondere in Bezug auf einen oder mehrere aus einem relativen Abstand, einer relativen Ausrichtung und einer Geste des Körperteils. Der relative Abstand und/oder die relative Ausrichtung kann in Bezug auf einen Sensor oder eine Kamera zur Erfassung von Bilddaten, wie z.B. den Sensor für sichtbares Licht, den Sensor für Nahinfrarotlicht und/oder die Laufzeitkamera, definiert werden. Zusammen mit optischen Merkmalen wie dem horizontalen und vertikalen Sichtfeld eines jeweiligen Sensors oder einer Kamera, insbesondere der Laufzeitkamera, können absolute metrische Werte des Körperteils wie Länge oder Breite der Finger oder Breite der Handfläche bestimmt werden. Die Genauigkeit der ermittelten charakteristischen geometrischen Körperteil-Eigenschaft wird weiter verbessert und daher wird die Rechenkomplexität weiter reduziert.

[0017] In einer Ausführungsform bezieht sich der Körperteil auf eine oder mehrere aus einer Handflächenseite und einer Handrückenseite. Die Authentifizierung kann auf Venenmustern, Handabdrücken und/oder Lebenslinien basieren. Die Authentifizierung basiert auf einem Körperteil, der viele Vorteile aufweist, wie z.B. leichte Zugänglichkeit, präzise Authentifizierung usw.

[0018] In einer Ausführungsform bezieht sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere aus einer Summe der Längen eines Fingersatzes einer Hand, einer Summe der durchschnittlichen Breiten eines Fingersatzes einer Hand und einer Breite einer Hand. Bei Männern und Frauen unterschiedlichen Alters ist

experimentell nachgewiesen worden, dass die Verwendung der Summe der Längen eines Fingersatzes einer Hand oder der Summe der durchschnittlichen Breiten der Finger einer Hand und der Breite einer Hand vorteilhafte Eigenschaften hat, wie z.B. leichte Bestimmbarkeit, leichte Zugänglichkeit, um den Vergleich mit vorgespeicherten biometrischen Merkmalen einzuschränken.

[0019] In einer Ausführungsform bezieht sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere aus einer linken Hand, einer rechten Hand, einer Handflächenseite und einer Handrückenseite. Eine Unterscheidung zwischen männlichen und weiblichen Händen kann ebenfalls bereitgestellt werden. Der Vergleich wird weiter beschränkt und die Rechenkomplexität weiter reduziert.

[0020] In einer Ausführungsform bezieht sich der Ähnlichkeitsgrad auf eine Unterteilung der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft in eine Vielzahl von Teilmengen. Nur der Vergleich biometrischer Merkmale einer relevanten Teilmenge oder einiger weniger relevanter Teilmengen ist erforderlich, und die Rechenkomplexität wird weiter reduziert.

[0021] In einer Ausführungsform überlappen die Teilmengen einander, insbesondere mit einem Spielraum entsprechend einem erwarteten Fehler der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft. Eine falsche Ablehnung der Authentifizierung kann vermieden werden, während die Zunahme der Rechenkomplexität begrenzt bleibt.

[0022] Mindestens eine Aufgabe der Erfindung wird auch durch ein biometrisches Authentifizierungsverfahren zur Authentifizierung einer Person durch Vergleich biometrischer Merkmale eines Körperteils der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen mehrerer registrierter Personen erreicht. Das biometrische Authentifizierungsverfahren umfasst: Erfassen von Bilddaten des Körperteils der Person; Bestimmen aus den erfassten Bilddaten mindestens einer charakteristischen geometrischen Körperteil-Eigenschaft des Körperteils der Person und biometrischer Merkmale des Körperteils der Person; Beschränken des Vergleichs der biometrischen Merkmale des Körperteils der Person auf vorgespeicherte biometrische Merkmale von Körperteilen der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft der Person aufweisen.

[0023] In einer Ausführungsform umfasst das biometrische Authentifizierungsverfahren ferner: Bereitstellen mindestens eines Sensors für sichtbares Licht, eines Sensors für Nahinfrarotlicht oder einer Laufzeitkamera zur Erfassung von Bilddaten.

[0024] In einer Ausführungsform umfasst das biometrische Authentifizierungsverfahren ferner: Bereitstellen einer Benutzerführung auf der Grundlage der mit der Laufzeitkamera aufgenommenen Bilddaten.

[0025] In einer Ausführungsform bezieht sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere aus der Summe der Längen eines Fingersatzes einer Hand und der Breite einer Hand.

[0026] In einer Ausführungsform bezieht sich der Ähnlichkeitsgrad auf eine Unterteilung der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft in eine Vielzahl von Teilmengen.

[0027] In einer Ausführungsform überlappen die Teilmengen einander, insbesondere mit einem Spielraum entsprechend einem erwarteten Fehler der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft.

KURZE ERLÄUTERUNG DER FIGUREN

[0028] Im Folgenden wird die Erfindung anhand von Ausführungsformen, die in den Figuren dargestellt sind, näher beschrieben. Die Figuren zeigen:

- | | |
|--------|---|
| Fig. 1 | illustriert schematisch die Handflächenseite der linken Hand einer ersten Person; |
| Fig. 2 | illustriert schematisch die Handflächenseite der rechten Hand einer zweiten Person; |
| Fig. 3 | illustriert schematisch das Venennetz der Rückseite der rechten Hand einer dritten Person; |
| Fig. 4 | illustriert schematisch die Hand einer Person und eine biometrische Authentifizierungsvorrichtung; |
| Fig. 5 | illustriert schematisch eine Laufzeitkamera; |
| Fig. 6 | illustriert schematisch charakteristische geometrische Handeigenschaften der Hand der ersten Person; |
| Fig. 7 | illustriert schematisch die Unterteilung eines durch charakteristische Handteileigenschaften definierten Raumes in Teilmengen; |
| Fig. 8 | illustriert schematisch die Schritte eines biometrischen Authentifizierungsverfahrens anhand von Teilmengen charakteristischer Handteileigenschaften; |
| Fig. 9 | illustriert schematisch die Schritte eines biometrischen Authentifizierungsverfahrens; und |

Fig. 10 illustriert schematisch die Schritte, die die Benutzerführung betreffen.

AUSFÜHRUNGSFORMEN DER ERFINDUNG

[0029] Figur 1 illustriert schematisch die Handflächenseite der linken Hand 1 einer ersten Person. Die linke Hand 1 hat einen Daumen t, einen Zeigefinger i, einen Mittelfinger m, einen Ringfinger r und einen kleinen Finger l. Figur 2 zeigt schematisch die Handflächenseite der rechten Hand 2 einer zweiten Person. Die rechte Hand 2 hat einen Daumen t, einen Zeigefinger i, einen Mittelfinger m, einen Ringfinger r und einen kleinen Finger l.

[0030] Figur 1 und Figur 2 zeigen schematisch Bilder der Handflächen der linken und rechten Hand 1, 2, die mit einem Sensor für sichtbares Licht (z. B. 400 nm bis 600 nm) aufgenommen wurden. Die Hände 1, 2 haben Handabdrücke P oder Lebenslinien, die im sichtbaren Licht identifiziert werden können. Zusätzlich oder alternativ können Venenmuster der Hände 1, 2 aus Bilddaten bestimmt werden, die im Nahinfrarotlicht (z.B. 700 nm bis 900 nm) aufgenommen wurden. Figur 1 und Figur 2 zeigen keine Venenmuster.

[0031] Wie in Figur 1 und Figur 2 illustriert, enthalten die Handabdrücke P oder Lebenslinien der Hände 1, 2 dieser beiden Personen individuelle biometrische Merkmale, wie bestimmte Längen, Positionen, Krümmungen usw. Durch den Vergleich mit biometrischen Merkmalen, die aus Körperteilen von registrierten Personen vorgespeichert wurden, wird die Authentifizierung einer bestimmten Person ermöglicht, - insbesondere in Kombination mit biometrischen Merkmalen, die aus entsprechenden Venenmustern ermittelt wurden. Darüber hinaus kann die Authentifizierung einer Person auch auf biometrischen Merkmalen des Handrückens beruhen, die aus Bilddaten bestimmt werden, die im sichtbaren Licht, im Nahinfrarotlicht oder einer Kombination davon erfasst wurden. Es ist jedoch derzeit nicht bekannt, ob biometrische Merkmale des Handrückens, die aus Bilddaten ermittelt wurden, die mit einem Sensor für sichtbares Licht erfasst wurden, eine ausreichende Authentifizierung einer Person ermöglichen. Wenn man auf den Handrücken angewiesen ist, wird gegenwärtig angenommen, dass mit einem Sensor für Nahinfrarotlicht erfasste Bilddaten notwendig sind, um die ausreichende Authentifizierung einer Person zu ermöglichen.

[0032] Figur 3 illustriert schematisch das Venennetz der Rückseite der rechten Hand 3 einer dritten Person. Die rechte Hand 3 hat einen Daumen t, einen Zeigefinger i, einen Mittelfinger m, einen Ringfinger r und einen kleinen Finger l. Wie in Figur 3 illustriert, umfasst die Rückseite der Hand 3 Venen, zu denen das dorsale Venennetz 31 (rete venosum dorsale manus) und die dorsalen Mittelhandvenen 32 (Vv. metacarpals dorsales) gehören. Venenmuster können aus Bilddaten bestimmt werden, die mit einem Sensor für Nahinfrarotlicht erfasst wurden, und individuelle biometrische Merkmale können aus den im Nahinfrarotlicht erfassten Bilddaten bestimmt werden.

[0033] Die Authentifizierung einer Person basiert auf vorgespeicherten biometrischen Merkmalen der Hände der registrierten Benutzer. Für jede registrierte Person enthält eine Datenbank biometrische Merkmale, die aus Bilddaten bestimmt werden, die im sichtbaren Licht, im Naheinfrarotlicht oder einer Kombination davon erfasst wurden. Die Bilddaten umfassen Bilddaten der Hand. Die Bilddaten können Bilddaten der Handfläche, des Handrückens oder eine Kombination davon enthalten. Die Bilddaten können Bilddaten der linken Hand, der rechten Hand oder eine Kombination davon enthalten. Um eine Person zu authentifizieren, werden Bilddaten von der Hand der Person erfasst. Die Bilddaten werden im sichtbaren Lichtspektrum, im Nahinfrarotlichtspektrum oder einer Kombination davon erfasst. Die Bilddaten können von der Handflächenseite, von der Handrückseite oder einer Kombination davon erfasst werden. Die Bilddaten können von der linken Hand, von der rechten Hand oder einer Kombination davon erfasst werden. Aus den erfassten Bilddaten werden die biometrischen Merkmale der betreffenden Person bestimmt und mit vorgespeicherten biometrischen Merkmalen der Datenbank verglichen. Im Falle einer Übereinstimmung wird die Authentifizierung genehmigt. Andernfalls wird die Authentifizierung abgelehnt. Der Vergleich aktueller biometrischer Merkmale einer Person mit vorgespeicherten biometrischen Merkmalen ist rechnerisch aufwendig, insbesondere dann, wenn sich die vorgespeicherten biometrischen Merkmale zum Beispiel auf mehr als 1.000 Personen beziehen. Aus Gründen der Benutzerfreundlichkeit sind jedoch für die Authentifizierung einer Person Antwortzeiten von weniger als 1 Sekunde erforderlich. Im Folgenden wird eine Technik zum Vergleich biometrischer Merkmale beschrieben, die es ermöglicht, die Rechenkomplexität z.B. um den Faktor 10 bis 13 zu reduzieren und damit ausreichend schnelle Antwortzeiten mit Standardcomputern zu ermöglichen.

[0034] Figur 4 illustriert schematisch eine biometrische Authentifizierungsvorrichtung 30. Die biometrische Authentifizierungsvorrichtung 30 umfasst einen biometrischen Sensor 10 und eine Verarbeitungseinheit 20. Die biometrische Authentifizierungsvorrichtung 30 kann zum Beispiel an ein Benutzerdisplay 40 angeschlossen werden, um eine Benutzerführung zu ermöglichen. Die Verarbeitungseinheit 20 kann an den biometrischen Sensor 10 angeschlossen werden, wie in Figur 4 illustriert. Die Verarbeitungseinheit 20 kann sich an einem entfernten Standort innerhalb einer Datenverarbeitungsinfrastruktur, wie einem Host-Computer, Server, einer Cloud usw., befinden. Die Verarbeitungseinheit 20 kann einen oder mehrere Prozessoren umfassen und kann über gespeicherte Computerbefehle verfügen, die von dem einen oder den mehreren Prozessoren ausgeführt werden können, um die in der vorliegenden Offenbarung beschriebenen Funktionen zu ermöglichen. Das Benutzerdisplay 40 kann fest in der Nähe des biometrischen Sensors 10 angeordnet werden. Das Benutzerdisplay 40 kann sich auf eine Benutzervorrichtung wie ein Notebook, ein Smartphone, eine Smartwatch usw. beziehen, wobei die Verarbeitungseinheit 20 zum Beispiel über eine drahtlose Verbindung wie z. B. Bluetooth mit dem Benutzerdisplay 40 kommunizieren kann. Die biometrische Authentifizierungsvorrichtung 30 kann in einer Benutzervorrichtung wie einem Notebook, Smartphone, einer Smartwatch usw. enthalten sein. Wie in Figur 4 dargestellt, kann eine

aktuelle Haltung der Hand des Benutzers 401 und eine gewünschte Haltung der Hand des Benutzers 402 auf dem Display 40 angezeigt werden.

[0035] Der biometrische Sensor 10 ermöglicht die Erfassung von Bilddaten der Hand 4 einer Person. Der biometrische Sensor 10 umfasst einen Sensor für sichtbares Licht 101 zur Erfassung von Bilddaten im sichtbaren Lichtspektrum, einen Sensor für Nahinfrarotlicht 102 zur Erfassung von Bilddaten im Nahinfrarotlichtspektrum und eine Laufzeitkamera 103 zur Erfassung von dreidimensionalen Bilddaten. Einer oder mehrere aus dem Sensor für das sichtbare Licht 101, dem Sensor für das Nahinfrarotlicht 102 und der Laufzeitkamera 103 können in einem einzigen Sensor enthalten sein. Darüber hinaus enthält der biometrische Sensor 10 Lichtquellen 104. Figur 4 illustriert acht Lichtquellen 104, die auf einem Kreis um die Sensoren 101, 102 und die Laufzeitkamera 103 angeordnet sind. Die Lichtquellen 104 können eine unterschiedliche Anzahl von Lichtquellen enthalten und/oder auf andere Weise angeordnet sein. Die Lichtquellen 104 können eine oder mehrere Lichtquellen enthalten, die Beleuchtung im sichtbaren Lichtspektrum bereitstellen und die Erfassung von Bilddaten mit dem Sensor für sichtbares Licht 101 im sichtbaren Lichtspektrum ermöglichen. Die Lichtquellen 104 können eine oder mehrere Lichtquellen enthalten, die für Beleuchtung im Nahinfrarotlicht sorgen und die Erfassung von Bilddaten mit dem Sensor für Nahinfrarotlicht 102 im Nahinfrarotlicht ermöglichen. Eine Kalibrierung kann insbesondere in Bezug auf die geometrische Lage des Sensors für sichtbares Licht 101, des Sensors für Nahinfrarotlicht 102 und der Laufzeitkamera 103 erfolgen, wie z.B. die translatorische Verschiebung zwischen dem Sensor für sichtbares Licht 101, dem Sensor für Nahinfrarotlicht 102 und der Laufzeitkamera 103. Darüber hinaus kann eine Kalibrierung in Bezug auf einen Skalierungsfaktor der von der Laufzeitkamera 103 erfassten Bilddaten, wie z.B. die absolute Größe der Objekte in den erfassten Bilddaten, vorgesehen werden. Die Kalibrierung kann innerhalb des biometrischen Sensors 10 durch Nachbearbeitung in einem dedizierten Computer wie der Verarbeitungseinheit 20 oder einer Kombination davon erfolgen. Die Kalibrierung kann vorsehen, dass die Objekte in den Bilddaten, die vom Sensor für sichtbares Licht 101, vom Sensor für Nahinfrarotlicht 102 und von der Laufzeitkamera 103 erfasst werden, zueinander ausgerichtet werden.

[0036] Der Sensor für sichtbares Licht 101 kann einen für sichtbares Licht empfindlichen Chip enthalten, der 2D-Bilddaten (2D: zweidimensional) entsprechend der Intensitätsverteilung des sichtbaren Lichts bereitstellt, die von einer 3D-Szene erzeugt wird (3D: dreidimensional). Der Nahinfrarotlichtsensor 102 kann einen für Nahinfrarotlicht empfindlichen Chip enthalten, der 2D-Bilddaten (2D: zweidimensional) entsprechend mit der Intensitätsverteilung des Nahinfrarotlichtes bereitstellt, die von einer 3D-Szene erzeugt wird (3D: dreidimensional). Der Sensor für sichtbares Licht 101 und der Sensor für Nahinfrarotlicht 102 können Linsen, Puffer, Regler, Verarbeitungselektronik usw. enthalten. Der Sensor für sichtbares Licht 101 und der Sensor für Nahinfrarotlicht 102 können sich auf kommerziell erhältliche Sensoren beziehen, wie z.B. auf den e2v-Halbleiter SAS EV76C570 CMOS-Bildsensor, der mit einem optischen Sperrfilter <500 nm Wellenlänge für den Sensor für sichtbares Licht 101 und mit einem optischen Sperrfilter von >700 nm für den Sensor für Nahinfrarotlicht 102 ausgestattet ist, oder wie z. B. den OmniVision OV4686 RGB-Ir-Sensor, wobei der Sensor für sichtbares Licht 101 und der Sensor für Nahinfrarotlicht 102 in einem Chip kombiniert sind und einen RGB-Ir-Filter enthalten). Die Lichtquellen 104 können einen Generator für sichtbares Licht und/oder Nahinfrarotlicht, wie z.B. eine LED (LED: lichtemittierende Diode), enthalten. Die Lichtquellen 104 können sich auf kommerziell erhältliche Lichtquellen beziehen, wie z.B. Hochleistungs-LEDs der Serie SMB1N von Roithner Laser Technik GmbH, Wien.

[0037] Figur 5 illustriert schematisch eine Laufzeitkamera 103. Die Laufzeitkamera 103 umfasst einen Sequenzregler 1031, einen Modulationsregler 1032, eine Pixelmatrix 1033, einen A/D-Wandler 1034 (A/D: analog zu digital), eine LED oder VCSEL 1035 (LED: lichtemittierende Diode; VCSEL: oberflächenemittierender Laser mit vertikalem Hohlraum) und ein Objektiv 1036. Der Sequenzregler steuert den Modulationsregler 1032 und den A/D-Wandler 1034.

[0038] Der Modulationsregler 1032 steuert die LED oder den VCSEL 1035 und die Pixelmatrix 1033. Die Pixelmatrix 1033 stellt dem A/D-Wandler 1034 Signale bereit. Der Sequenzregler 1031 interagiert mit einem Host-Regler 1037, zum Beispiel über den I²C-Bus (I²C: I-Squared-C serial data bus). Die LED oder der VCSEL 1035 beleuchten eine 3D-Szene 1038. Nach einer Laufzeit empfängt das Objektiv 1036 das von der 3D-Szene 1038 reflektierte Licht. Der A/D-Wandler 1034 stellt dem Host-Regler 1037 rohe 3D-Bilddaten (3D: dreidimensional) bereit, zum Beispiel über die MIPI CSI-2 oder PIF (MIPI: Mobile Industrie-Prozessor-Schnittstelle; CSI: serielle Kameraschnittstelle; PIF (MIPI: Mobile Industry Processor Interface): parallele Schnittstelle). Der Host-Regler führt eine Tiefenkartenberechnung durch und stellt ein Amplitudenbild 103a der 3D-Szene 1038 und ein Tiefenbild 103d der 3D-Szene bereit. Wie in Figur 5 illustriert, enthält der Hintergrund des Amplitudenbildes 103a zum Beispiel Lichtschatten einer Wand hinter einer Person, während der Hintergrund des Tiefenbildes 103d einen einzigen Wert, z.B. schwarz, hat, weil die Wand hinter der Person in einem bestimmten Abstand zur Laufzeitkamera 103 angeordnet ist. Die Laufzeitkamera 103 kann sich auf eine REAL3™ der Firma Infineon™ beziehen, und kann die folgenden Spezifikationen umfassen: direkte Messung von Tiefe und Amplitude in jedem Pixel; höchste Genauigkeit; geringe Rechenlast; aktiv modulierte Infrarotlicht und patentierte SBI-Schaltung (Suppression of Background Illumination) in jedem Pixel; volle Funktionsfähigkeit bei allen Lichtverhältnissen: Dunkelheit und helles Sonnenlicht; monokulare Systemarchitektur ohne mechanische Grundlinie; kleinste Größe und hohe Designflexibilität; keine Einschränkung beim Betrieb im Nahbereich; keine besonderen Anforderungen an die mechanische Stabilität; keine mechanische Ausrichtung und Winkelkorrektur; keine Rekalibrierung oder Gefahr der De-Kalibrierung durch Stürze, Vibrationen oder thermische Biegung; einfache und sehr schnelle einmalige Kalibrierung; kosteneffiziente Herstellung.

[0039] Wie weiter unten erläutert wird, stellt die biometrische Authentifizierungsvorrichtung 30, wie in Figur 5 dargestellt, die Authentifizierung einer Person durch den Vergleich biometrischer Merkmale einer Hand 4 der Person mit vorgespei-

cherten biometrischen Merkmalen der Hände mehrerer registrierter Personen bereit. Die biometrische Authentifizierungsvorrichtung 30 ist so konfiguriert, dass sie Bilddaten der Hand 4 der Person erfasst, aus den erfassten Bilddaten mindestens eine charakteristische geometrische Handeigenschaft S_f , W_h der Hand 4 der Person und biometrische Merkmale der Hand 4 der Person bestimmt und den Vergleich der biometrischen Merkmale der Hand 4 der Person auf vorgeschaltete biometrische Merkmale von Händen der Vielzahl der registrierten Personen beschränkt, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Handeigenschaft S_f , W_h der Person aufweisen.

[0040] Die biometrische Authentifizierungsvorrichtung kann so konfiguriert werden, dass sie abwechselnd Bilddaten im sichtbaren Lichtspektrum und Bilddaten im Nahinfrarotlichtspektrum erfasst. Die Lichtsensoren 104 können so konfiguriert werden, dass sie dementsprechend abwechselnd Beleuchtung im sichtbaren Lichtspektrum und Beleuchtung im Nahinfrarotlichtspektrum bereitstellen.

[0041] Figur 6 illustriert schematisch charakteristische geometrische Handeigenschaften der Hand 1 der ersten Person, die auf der Grundlage von Bilddaten bestimmt werden können, die zum Beispiel von der Laufzeitkamera 103 erfasst wurden. Die von der Laufzeitkamera 103 erfassten Bilddaten sind kalibriert und ermöglichen eine genaue Vermessung und Kartierung der Hand 1 der ersten Person auf der Grundlage eines geometrischen Rasters R oder Netzes, das in Figur 6 mit gestrichelten Linien dargestellt ist. Mit Hilfe des Rasters R können die Längen L_i , L_m , L_r , L_1 der Finger bestimmt werden, die Breite W_h der Hand kann bestimmt werden, die Breiten W_{i1} , W_{i2} , W_{m1} , W_{m2} usw. der Fingerknochen können bestimmt werden, usw. Demnach lässt sich die Summe $S_f = L_i + L_m + L_r + L_1$ der Längen der vier Finger Zeigefinger i , Mittelfinger m , Ringfinger r und Kleinfinger 1 sowie die Breite W_h der Hand 1 der ersten Person bestimmen. Außerdem kann die Summe $W_f = (W_{i1} + W_{i2})/2 + (W_{m1} + W_{m2})/2 +$ usw. der mittleren Breiten der vier Finger Zeigefinger i , Mittelfinger m , Ringfinger r und kleiner Finger 1 der Hand bestimmt werden.

[0042] Wie in Figur 6 dargestellt, enthält das Raster R oder Netz für jeden der Finger i , m , r , 1 Referenzpunkte ri_1 , ri_2 , rm_1 , rm_2 , rr_1 , rr_2 , rl_1 , rl_2 am Ende und an der Wurzel jedes Fingers. Außerdem umfasst das Raster R oder Netz in Richtung von der Wurzel des Zeigefingers i zur Wurzel des kleinen Fingers 1 Referenzpunkte ri , rim , rmr , rrl , rl . In Figur 6 sind die Referenzpunkte ri_1 , ri_2 , rm_1 , ..., ri , rim , rmr usw. mit einem dicken schwarzen Kreis markiert, aber zur besseren Lesbarkeit enthalten nicht alle Referenzpunkte das jeweilige Bezugszeichen. Die Bestimmung der Referenzpunkte basiert auf Bildverarbeitungstechniken wie der Verwendung der OpenCV-Funktion „findContours“ und anderen. In Übereinstimmung mit den Referenzpunkten ri_1 , ri_2 , rm_1 , ..., ri , rim , rmr usw. ist das Raster R oder Netz klar definiert und die jeweiligen Längen oder Breiten der Finger oder der Hand können eindeutig bestimmt werden.

[0043] Figur 7 illustriert schematisch die Unterteilung des durch die charakteristischen Handteileigenschaften Hand mit W_h und Summe der Länge der vier Finger S_f definierten Raumes in Teilmengen T_i . Die Hand mit W_h ist einer ersten Koordinate oder Abszisse eines kartesischen Koordinatensystems zugeordnet. Die Summe der Länge der vier Finger S_f wird einer zweiten Koordinate oder Ordinate des kartesischen Koordinatensystems zugeordnet. Die Einheit der Abszisse und der Ordinate sind Millimeter [mm]. Werte der Breite W_h und der Summe S_f , die sich auf vorgeschaltete biometrische Merkmale von registrierten Personen beziehen, sind mit kleinen schwarzen Rauten markiert. Das kartesische Koordinatensystem ist in überlappende Teilmengen T_i unterteilt, wobei jede Teilmenge T_i eine rechteckige Form hat. Die überlappenden Teile der Teilmengen T_i sind dunkelgrau dargestellt, während die nicht überlappenden Teile der Teilmengen T_i hellgrau markiert sind. Der überlappende Bereich kann in Übereinstimmung mit einem erwarteten Messfehler zur Bestimmung der Breite W_h und der Summe S_f gewählt werden.

[0044] Wie in Figur 7 dargestellt, definieren die charakteristischen Handteileigenschaften W_h , S_f 2-dimensionale Intervalle $0 \dots 18$. Für den Fall, dass nicht nur zwei, sondern n charakteristische Handteileigenschaften betroffen sind, werden n -dimensionale Intervalle definiert. Jeder Satz biometrischer Merkmale einer bestimmten Hand wird den jeweiligen charakteristischen geometrischen Eigenschaften zugeordnet, was im Falle der in Figur 7 dargestellten zweidimensionalen Intervalle mindestens ein oder maximal vier Intervalle umfasst. Bei bekannten charakteristischen Handteileigenschaften ist bekannt, für welche Intervalle die jeweiligen biometrischen Merkmale verglichen werden müssen. Die Größe der Intervalle und damit die Anzahl der Intervalle hängen von der Reproduzierbarkeit der Eingabewerte ab, nämlich den charakteristischen Handteileigenschaften. Anstelle eines „Brute-force“-Abgleichs innerhalb solcher Intervalle kann eine weitere Optimierung erreicht werden, indem die Kandidaten nach ihrem Abstand sortiert werden und mit dem kleinsten Abstand begonnen wird, wobei davon ausgegangen wird, dass die charakteristischen Handteileigenschaften mit den biometrischen Merkmalen korrelieren.

[0045] Der Wert der Breite W_h und die Summe S_f einer Person, für die eine Authentifizierung erforderlich ist, wird mit einer großen weißen Raute markiert. Aufgrund von Messfehlern, die es sehr schwierig machen, eine Person nur auf der Grundlage der Breite W_h und der Summe S_f zu authentifizieren, stimmt die große weiße Raute nicht mit einer der schwarzen Raute überein, die sich auf die vorgeschalteten biometrischen Merkmale der registrierten Personen beziehen. Dementsprechend ist eine Authentifizierung auf der Grundlage eines Vergleichs biometrischer Merkmale erforderlich. Um die Person zu authentifizieren, reicht es jedoch aus, nur biometrische Merkmale der Person mit vorgeschalteten biometrischen Merkmalen von Personen zu vergleichen, die sich auf die jeweilige Teilmenge T_i beziehen. Abhängig von der Lage der weißen Raute beschränkt sich der Vergleich auf eine einzige Teilmenge T_i oder auf maximal vier Teilmengen T_i . In dem in Figur 7 illustrierten Beispiel beschränkt sich der Vergleich auf die beiden Teilmengen T_i , die die Breite W_h von 70 mm und die Summe S_f von 260 mm und 300 mm umfassen. Somit ist die Authentifizierung der Person auf vorgeschaltete biometrische Merkmale der Hände der Vielzahl registrierter Personen beschränkt, die ein vordefiniertes Ähnlichkeitsgrad

mit mindestens einem charakteristischen geometrischen Merkmal der Hand aufweisen, nämlich der Breite Wh und der Summe Sf. Dementsprechend wird die Rechenkomplexität für den Vergleich biometrischer Merkmale reduziert, beispielsweise um den Faktor 10 bis 13, wodurch ausreichend schnelle Antwortzeiten mit Standardcomputern ermöglicht werden.

[0046] Neben der Summe aus der Länge der vier Finger Sf und der Breite der Hand Wh kann sich eine charakteristische geometrische Handeigenschaft auf die Summe Wf der durchschnittlichen Breiten der vier Finger der Hand beziehen. Die charakteristische geometrische Handeigenschaft kann eine oder mehrere der folgenden Eigenschaften umfassen: die Summe Sf, die Breite Wh und die Summe Wf. So kann sich die in Figur 7 dargestellte Unterteilung auf einen eindimensionalen Raum, einen zweidimensionalen Raum oder einen dreidimensionalen Raum beziehen.

[0047] Neben der Summe aus der Länge der vier Finger Sf und der Breite der Hand Wh kann eine charakteristische geometrische Handeigenschaft mit der Krümmung der Hand und der Lage des Daumens zusammenhängen. Anhand der Krümmung der Hand lässt sich feststellen, ob sich die Bilddaten auf die Handfläche oder auf den Handrücken beziehen. Zusätzlich ermöglicht die Position des Daumens die Bestimmung, ob sich die Bilddaten auf die linke Hand oder die rechte Hand beziehen. Dementsprechend kann der Vergleich der biometrischen Merkmale auf die jeweiligen vorgeschicherten biometrischen Merkmale beschränkt werden, zum Beispiel auf die vorgeschicherten biometrischen Merkmale, die sich auf die Rückseite der linken Hand beziehen, auf die vorgeschicherten biometrischen Merkmale, die sich auf die Handfläche der linken Hand beziehen, usw. Folglich wird die Rechenkomplexität für den Vergleich biometrischer Merkmale reduziert.

[0048] Bei Betrachtung von Figur 4 kann die biometrische Authentifizierungsvorrichtung 30 eine Benutzerführung auf der Grundlage von Bilddaten bereitstellen, die mit der Laufzeitkamera 103 erfasst wurden. Die Benutzerführung kann sich auf das Bewegen der Hand 4 in eine vordefinierte Haltung beziehen. Die vordefinierte Haltung kann sich auf eine Haltung relativ zum biometrischen Sensor 10 beziehen. Wie in Figur 4 illustriert, kann eine aktuelle Haltung der Hand des Benutzers 401 und eine gewünschte Haltung der Hand des Benutzers 402 auf dem Display 40 angezeigt werden. Die Größe der angezeigten aktuellen Haltung der Hand des Benutzers 401 kann dem Benutzer eine Führung in Bezug auf den gewünschten relativen Abstand zum biometrischen Sensor 10 geben. Wenn beispielsweise die Größe der angezeigten aktuellen Haltung der Hand 401 des Benutzers kleiner ist als die Größe der angezeigten gewünschten Haltung der Hand 402 des Benutzers, wird der Benutzer angewiesen, die Hand 4 näher an den biometrischen Sensor 10 zu bewegen. Eine ähnliche Führung kann in Bezug auf die relative Ausrichtung der Hand 4 gegeben werden. Die relative Ausrichtung der Hand 4 kann sich auf eine Neigung der Handfläche oder des Handrückens in Bezug auf eine durch den biometrischen Sensor 10 definierte Ebene beziehen. Ähnliche Führungen können in Bezug auf eine Geste der Hand gegeben werden. Die Geste der Hand kann sich auf das Spreizen der Finger, auf das Strecken der Finger usw. beziehen.

[0049] Figur 8 illustriert schematisch die Schritte eines biometrischen Authentifizierungsverfahrens zur Authentifizierung einer Person durch den Vergleich biometrischer Merkmale einer Hand 4 der Person mit vorgeschicherten biometrischen Merkmalen von Hand s einer Vielzahl registrierter Personen. In Schritt S1 werden die Bilddaten der Hand 4 der Person erfasst. Im Schritt S2 werden aus den erfassten Bilddaten mindestens eine charakteristische geometrische Handeigenschaft Sf, Wh der Hand 4 der Person und biometrische Merkmale der Hand 4 der Person bestimmt. Bestimmt werden insbesondere Teilmengenzahlen gemäß den in Verbindung mit Figur 7 definierten Intervallen. In Schritt S3 wird der Vergleich der biometrischen Merkmale der Hand 4 der Person mit vorgeschicherten biometrischen Merkmalen der Hand s der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Handeigenschaft Sf, Wh der Person aufweisen, insbesondere in Übereinstimmung mit der/den bestimmten Teilmenge(n), beschränkt.

[0050] Figur 9 illustriert schematisch die Bausteine der algorithmischen Kette zur Authentifizierung einer Person. Im Schritt Sa1 werden Bilddaten mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 aufgenommen, wobei der Sensor für sichtbares Licht 101, der Sensor für Nahinfrarotlicht 102, die Laufzeitkamera 103 und die Lichtquellen 104 jeweils geregelt werden. Bilddaten können im gemeinsamen Speicher oder in einem Dateisystem gespeichert werden. In Schritt Sa2 wird der Hintergrund aus den Bilddaten eliminiert, die mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 aufgenommen wurden. In Schritt Sa3 wird in den Bilddaten, die mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 aufgenommen wurden, ein interessierender Bereich (ROI) bestimmt. In Schritt Sa4 werden Bildverbesserungen oder Filter auf Bilddaten angewendet, die mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 erfasst wurden. Verbesserungen oder Filter können sich auf Unschärfmaskierung, adaptive Schwellenmessungen, Laplace-Transformation usw. in Schritt Sa5 beziehen, biometrische Merkmale werden aus Bilddaten extrahiert, die mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 aufgenommen wurden. Die Extraktion von Bildmerkmalen kann sich auf ORB (Oriented FAST and Rotated BRIEF), SIFT (Scale-Invariant Feature Transform), SURF (Speeded-Up Robust Features) usw. beziehen. Im Schritt Sa6 erfolgt der Abgleich biometrischer Merkmale auf der Grundlage biometrischer Merkmale, die aus den mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 aufgenommenen Bilddaten extrahiert werden. Der Abgleich biometrischer Merkmale kann BF (Brute Force), FLANN (Fast Approximate Nearest Neighbor Search) usw. umfassen. In Schritt Sa7 werden Personen- und Terminalidentifikation verifiziert und entsprechend eine JA/NEIN-Entscheidung getroffen. Abhängig von der Art der Merkmalsdeskriptoren werden n-dimensionale Merkmalsvektoren üblicherweise unter Verwendung der euklidischen Distanz (oder L2-Norm) verglichen und abgeglichen, während binär kodierte Merkmale unter Verwendung der Hamming-Distanz verglichen und abgeglichen werden.

[0051] Figur 10 illustriert schematisch die Schritte, die für die Bereitstellung einer Benutzerführung in Bezug auf das Anleiten einer Person erforderlich sind, um die Hand 4 in eine gewünschte Haltung in Bezug auf die biometrische Authentifizierungsvorrichtung 30 zu bringen. In Schritt Sg1 wird mit Hilfe der Laufzeitkamera 103 überprüft, ob sich ein Objekt in einer Entfernung von zum Beispiel 40 cm befindet. Wenn nicht, wird Schritt Sg1 nach einer vordefinierten Verzögerung, wie vorzugsweise 200 Millisekunden, wiederholt. In Schritt Sg2 wird mit der Laufzeitkamera 103 überprüft, ob das Objekt die Form einer Hand hat. Wenn nicht, wird nach einer vordefinierten Verzögerung von zum Beispiel zwischen einer Sekunde und fünf Sekunden, vorzugsweise drei Sekunden, Schritt Sg1 wiederholt. Im Schritt Sg3 werden auf der Grundlage von Bilddaten, die mit der Laufzeitkamera 103 aufgenommen wurden, die absoluten Abmessungen der Hand bestimmt. In Schritt Sg4 wird eine Darstellung der Hand auf einem Display 40 in einer gewünschten Position angezeigt, die für den Sensor für sichtbares Licht 101 und den Sensor für Nahinfrarotlicht 102 optimal ist, wobei sich diese Position in einem vordefinierten Abstand von beispielsweise etwa k cm befindet, wobei k innerhalb des Tiefenschärfebereichs des Sensors für sichtbares Licht 101 und/oder des Sensors für Nahinfrarotlicht 102 liegt. Die Darstellung der Hand wird mit nur leicht gespreizten Fingern dargestellt. In Schritt Sg5 wird die aktuelle Position der Hand kontinuierlich mit Hilfe der Laufzeitkamera 103 bestimmt und eine Darstellung der aktuellen Position der Hand kontinuierlich auf dem Display 40 angezeigt, insbesondere zusammen mit einer Überlagerung einer Libelle, die die Drehung oder Neigung der Hand in Bezug auf die gewünschte Position anzeigt. In Schritt Sg6 wird überprüft, ob sich die Hand in der gewünschten Position befindet, insbesondere hinsichtlich des gewünschten vordefinierten Abstands zum Sensor für sichtbares Licht 101 und zum Sensor für Nahinfrarotlicht 102. Wenn nicht, geht es mit Schritt Sg5 weiter. Andernfalls wird in Schritt Sg7 die Darstellung der Hand an der gewünschten Position in eine Hand mit gespreizten Fingern, nämlich in eine Hand mit einer gewünschten Geste, umgewandelt, und die Darstellung der Hand an der aktuellen Position wird auf der Grundlage von Bilddaten, die mit dem Laufzeit-Sensor 103 aufgenommen wurden, kontinuierlich angezeigt. Befindet sich die Hand im Schritt Sg8 im optimalen Abstand (z.B. innerhalb von ± 3 cm), und befindet sich die Hand in einem optimalen Drehbereich (z.B. innerhalb von $\pm 12^\circ$) und in einem optimalen Neigungsbereich (z.B. innerhalb von $\pm 12^\circ$), werden die Bilddaten mit dem Sensor für sichtbares Licht 101 und dem Sensor für Nahinfrarotlicht 102 zur Authentifizierung der Person erfasst, z.B. gemäß den in Verbindung mit Figur 9 angegebenen Schritten. Die Benutzerführung ist dann beendet. Wenn in Schritt Sg8 Bilddaten nicht erfasst werden können, wird die Benutzerführung nach einer vordefinierten Zeitspanne, wie z.B. vorzugsweise vier Sekunden, unterbrochen, wobei entsprechende Informationen auf dem Display 40 so angezeigt werden, dass die Benutzerführung bei Schritt Sg1 wieder beginnt.

BEZUGSZEICHEN

[0052]

1, 2, 3	Hand der ersten, zweiten und dritten Person
t, i, m, r, 1	Daumen, Zeigefinger, Mittelfinger, Ringfinger, kleiner Finger
P	Handabdruck oder Lebenslinien
31, 32	dorsales Venennetz, dorsale Mittelhandvenen
4	Hand einer Person
10	biometrischer Sensor
101	Sensor für sichtbares Licht
102	Sensor für Nahinfrarotlicht
103	Laufzeitkamera
104	Lichtquellen
20	Verarbeitungseinheit
30	biometrische Authentifizierungsvorrichtung
40	Display
401, 402	aktuelle Haltung der Hand des Benutzers, gewünschte Haltung der Hand des Benutzers

Patentansprüche

1. Biometrische Authentifizierungsvorrichtung (30) zum Authentifizieren einer Person durch Vergleich biometrischer Merkmale eines Körperteils (4) der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen einer Vielzahl von registrierten Personen, wobei die biometrische Authentifizierungsvorrichtung (30) konfiguriert ist zum: Erfassen von Bilddaten des Körperteils (4) der Person; Bestimmen aus den erfassten Bilddaten mindestens einer charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) des Körperteils (4) der Person, und biometrischer Merkmale des Körperteils (4) der Person; Beschränken des Vergleichs der biometrischen Merkmale des Körperteils (4) der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) der Person aufweisen.

2. Biometrische Authentifizierungsvorrichtung (30) nach dem vorhergehenden Anspruch, die ferner so konfiguriert ist, dass sie Bilddaten mit mindestens einem Sensor für sichtbares Licht (101), einem Sensor für Nahinfrarotlicht (102), einem kombinierten Sensor für sichtbares Licht und Nahinfrarotlicht (101, 102) und einer Laufzeitkamera (103) erfasst.
3. Biometrische Authentifizierungsvorrichtung (30) nach dem vorhergehenden Anspruch, die ferner so konfiguriert ist, dass sie eine Benutzerführung auf der Grundlage der mit der Laufzeitkamera (103) erfassten Bilddaten bereitstellt.
4. Biometrische Authentifizierungsvorrichtung (30) nach dem vorhergehenden Anspruch, wobei sich die Benutzerführung auf das Bewegen des Körperteils (4) in eine vordefinierte Haltung bezieht, insbesondere in Bezug auf einen oder mehrere relative Abstände, eine relative Ausrichtung und eine Geste des Körperteils.
5. Biometrische Authentifizierungsvorrichtung (30) nach einem der vorhergehenden Ansprüche, wobei sich der Körperteil (4) auf eine oder mehrere Handflächenseiten und einen Handrücken bezieht.
6. Biometrische Authentifizierungsvorrichtung (30) nach einem der vorhergehenden Ansprüche, wobei sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere der folgenden Eigenschaften bezieht: eine Summe der Längen eines Satzes von Fingern einer Hand (Sf), eine Summe der durchschnittlichen Breiten eines Satzes von Fingern einer Hand (Wf) und eine Breite einer Hand (Wh).
7. Biometrische Authentifizierungsvorrichtung (30) nach einem der vorhergehenden Ansprüche, wobei sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere einer linken Hand, einer rechten Hand, einer Handflächenseite und einer Handrückenseite bezieht.
8. Biometrische Authentifizierungsvorrichtung (30) nach einem der vorhergehenden Ansprüche, wobei sich der Ähnlichkeitsgrad auf eine Unterteilung der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) in eine Vielzahl von Teilmengen (Ti) bezieht.
9. Biometrische Authentifizierungsvorrichtung (30) nach dem vorhergehenden Anspruch, wobei die Teilmengen (Ti) einander überlappen, insbesondere mit einem Spielraum entsprechend einem erwarteten Fehler der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wh).
10. Biometrisches Authentifizierungsverfahren zum Authentifizieren einer Person durch Vergleich biometrischer Merkmale eines Körperteils (4) der Person mit vorgespeicherten biometrischen Merkmalen von Körperteilen einer Vielzahl registrierter Personen, wobei das biometrische Authentifizierungsverfahren umfasst:
Erfassen von Bilddaten des Körperteils (4) der Person;
Bestimmen aus den erfassten Bilddaten
mindestens einer charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) des Körperteils (4) der Person und
biometrischer Merkmale des Körperteils (4) der Person;
Beschränken des Vergleichs der biometrischen Merkmale des Körperteils (4) der Person auf vorgespeicherte biometrische Merkmale von Körperteilen der Vielzahl registrierter Personen, die einen vordefinierten Ähnlichkeitsgrad mit der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) der Person aufweisen.
11. Biometrisches Authentifizierungsverfahren nach Anspruch 10, ferner umfassend: Bereitstellen mindestens eines aus einem Sensor für sichtbares Licht (101), einem Sensor für Nahinfrarotlicht (102) und einer Laufzeitkamera (103) zum Erfassen von Bilddaten.
12. Biometrisches Authentifizierungsverfahren nach Anspruch 10 oder 11, ferner umfassend: Bereitstellen einer Benutzerführung auf der Grundlage der mit der Laufzeitkamera (103) aufgenommenen Bilddaten.
13. Biometrisches Authentifizierungsverfahren nach einem der Ansprüche 10 bis 12, wobei sich die mindestens eine charakteristische geometrische Körperteil-Eigenschaft auf eine oder mehrere der folgenden Eigenschaften bezieht: eine Summe der Längen eines Satzes von Fingern einer Hand (Sf), eine Summe der durchschnittlichen Breiten eines Satzes von Fingern einer Hand (Wf) und eine Breite einer Hand (Wh).
14. Biometrisches Authentifizierungsverfahren nach einem der Ansprüche 10 bis 13, wobei sich der Ähnlichkeitsgrad auf eine Unterteilung der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh) in eine Vielzahl von Teilmengen (Ti) bezieht.
15. Biometrisches Authentifizierungsverfahren nach dem vorhergehenden Anspruch, wobei die Teilmengen (Ti) einander überlappen, insbesondere mit einem Spielraum entsprechend einem erwarteten Fehler der mindestens einen charakteristischen geometrischen Körperteil-Eigenschaft (Sf, Wf, Wh).

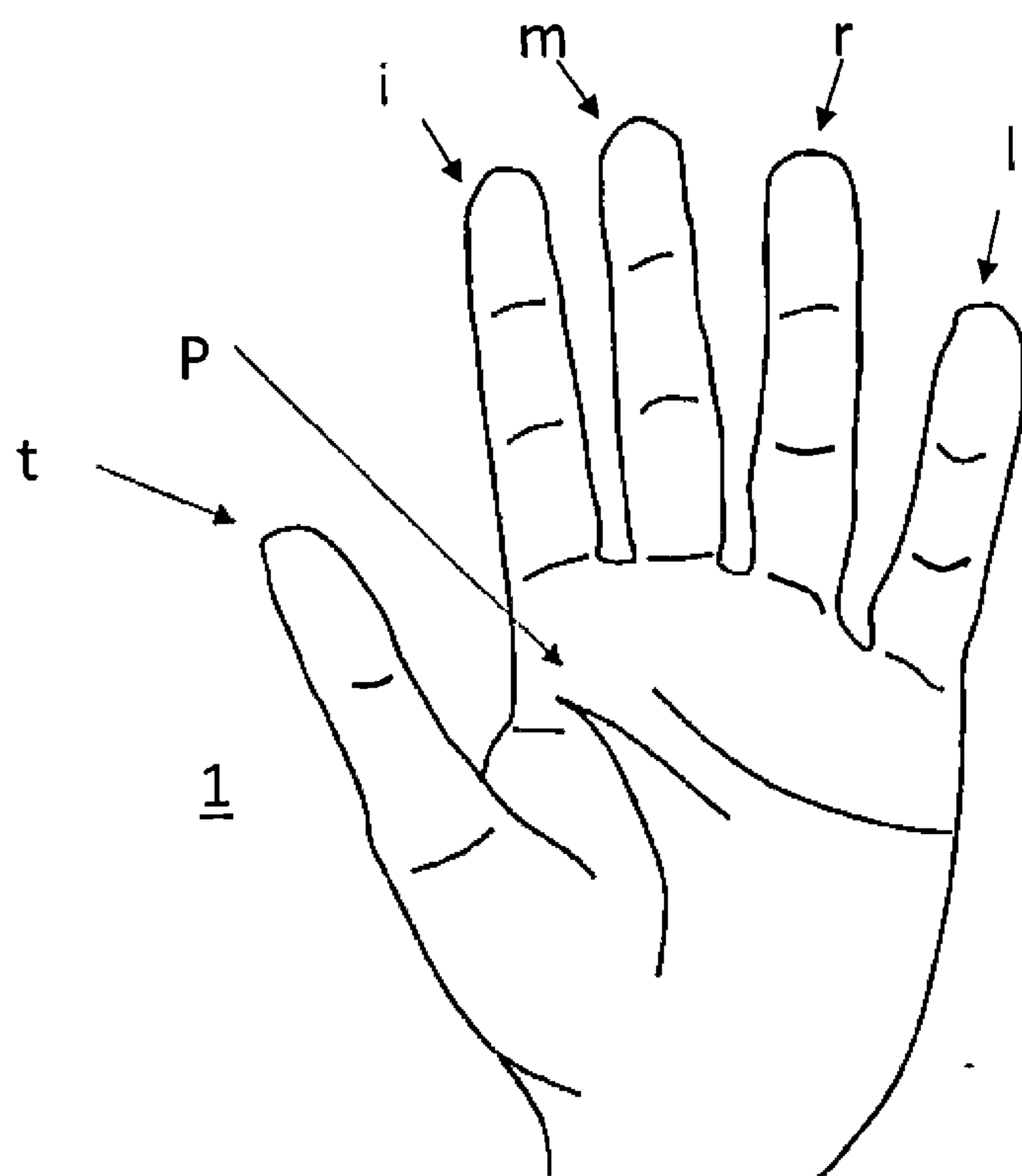


Fig. 1

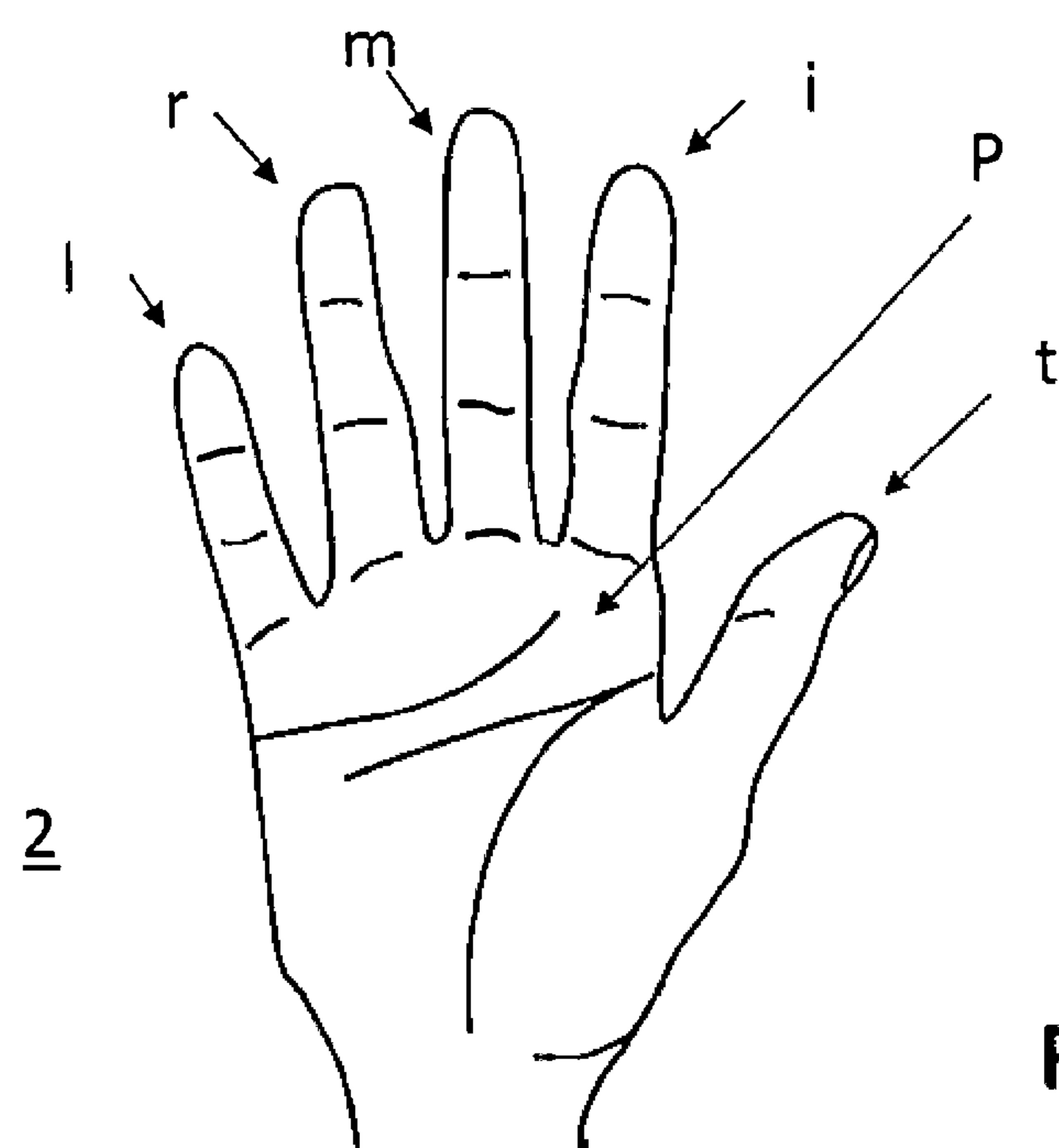


Fig. 2

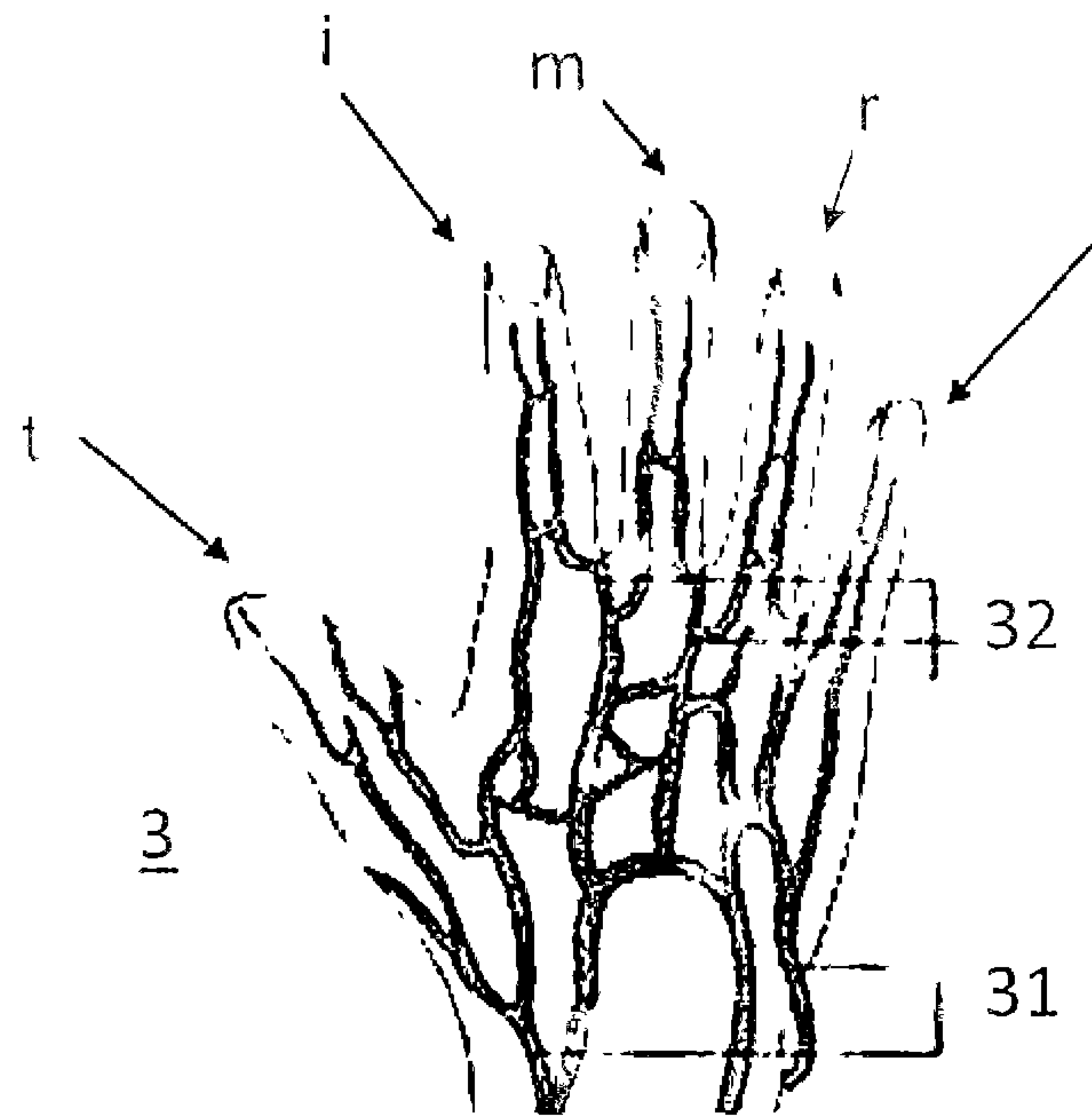


Fig. 3

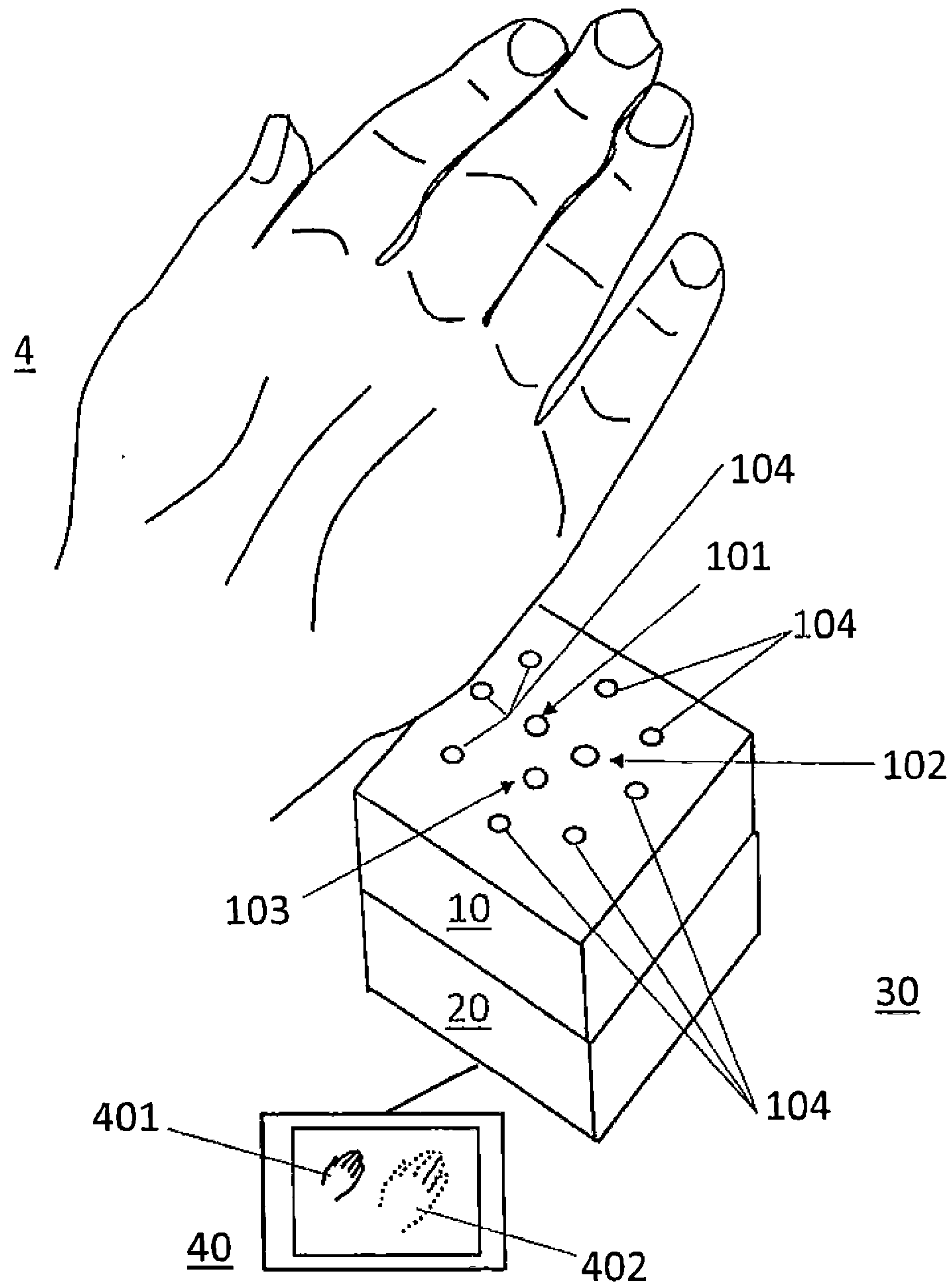


Fig. 4

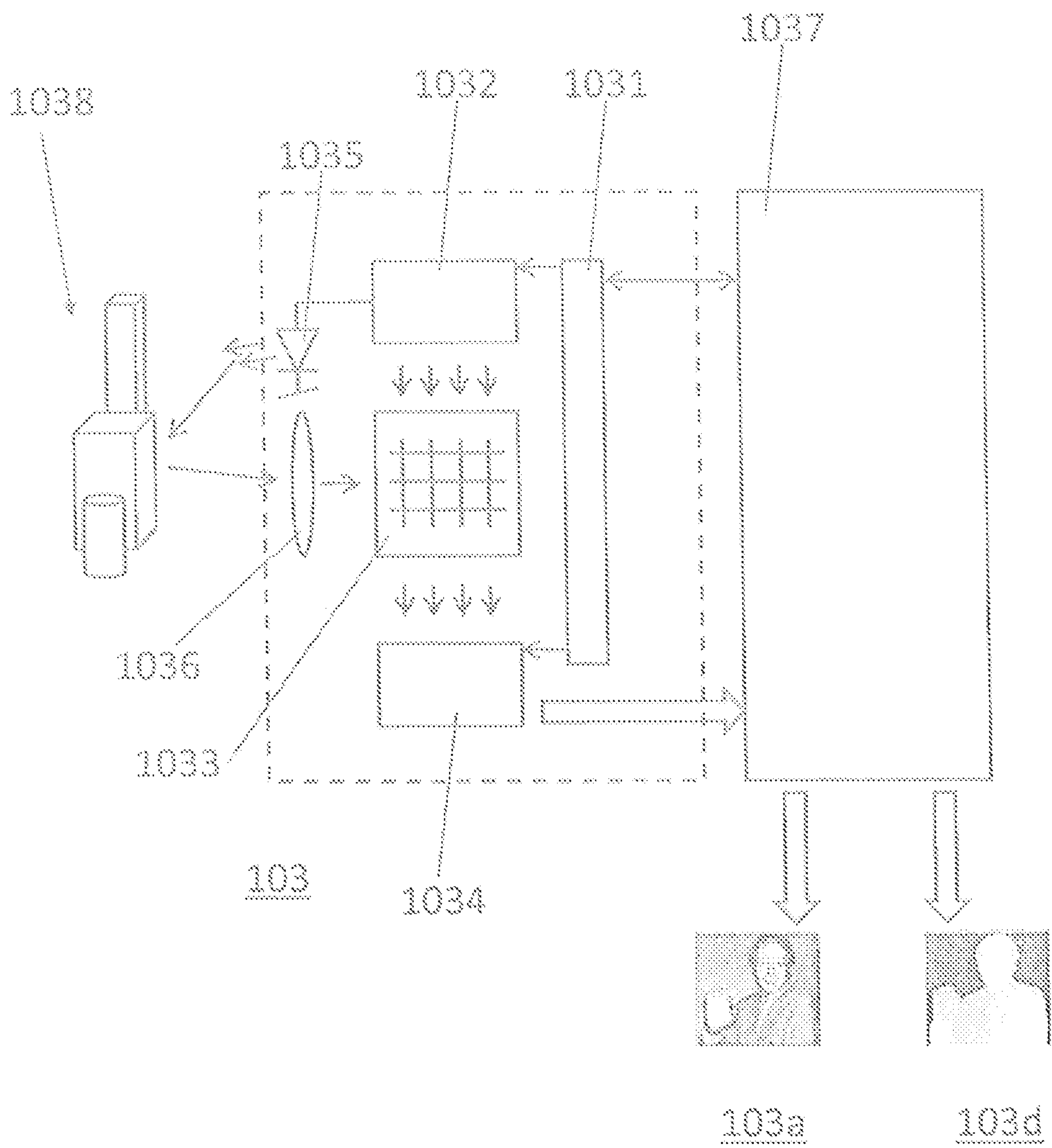


Fig. 5

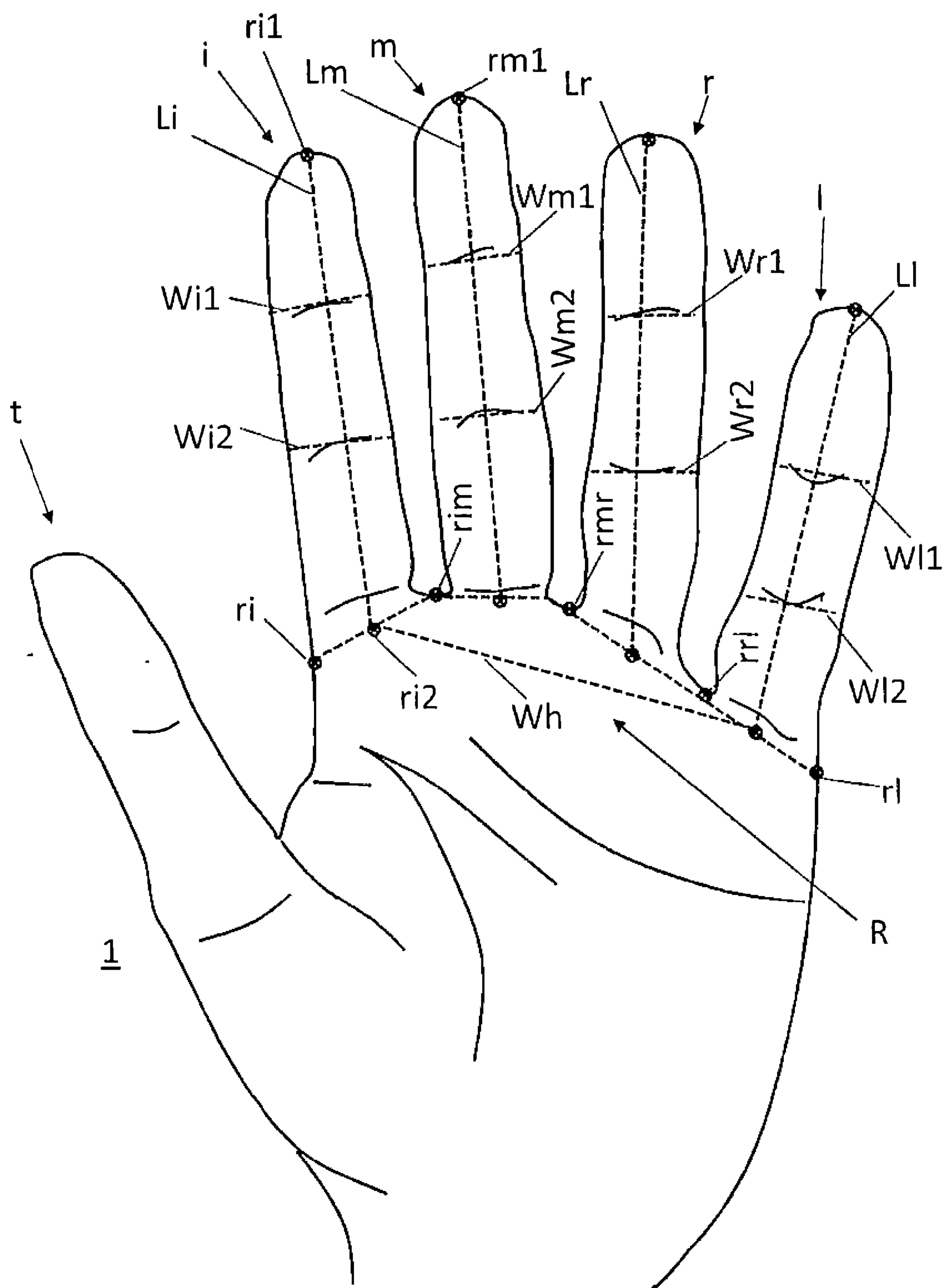
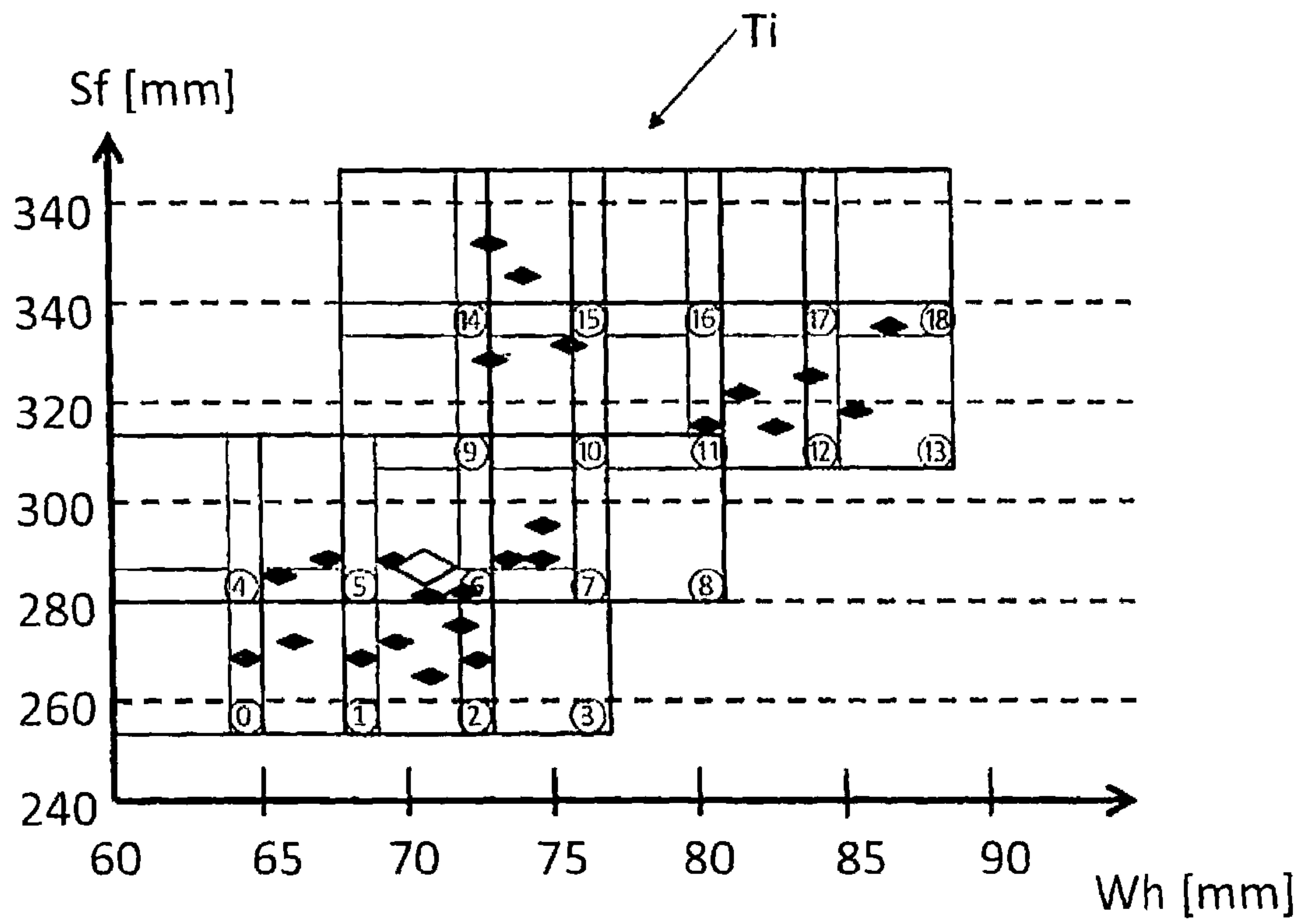
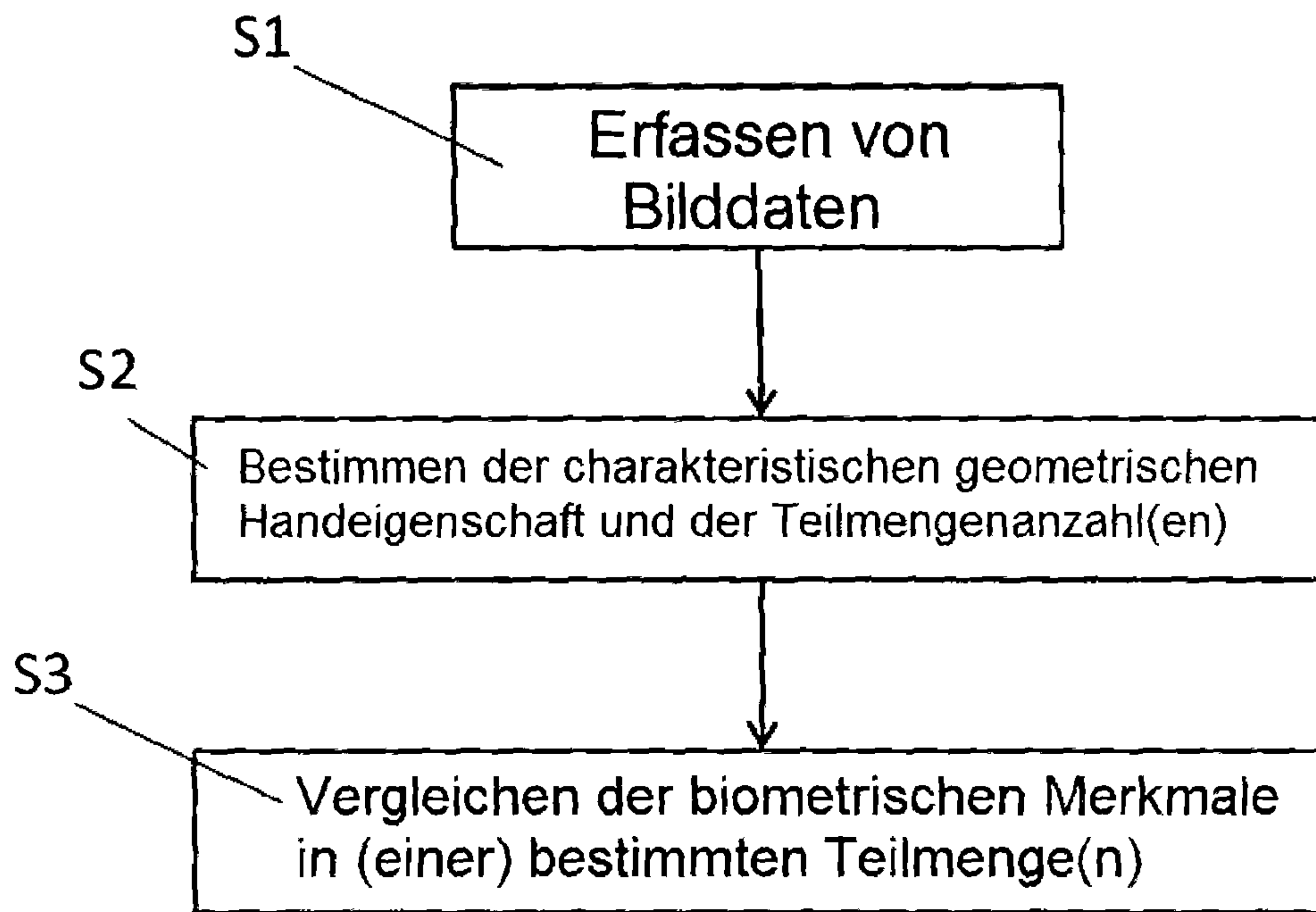
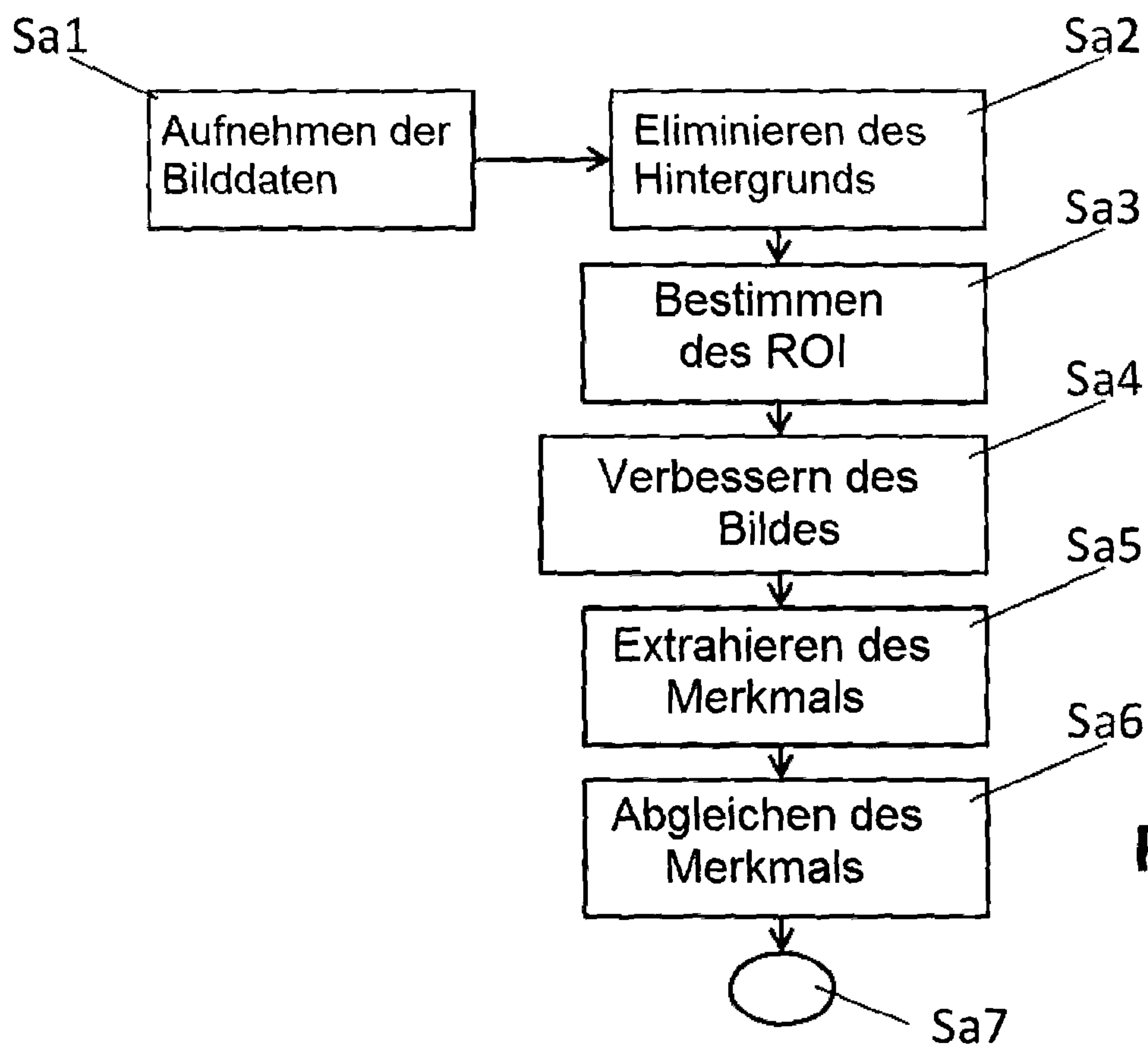


Fig. 6

**Fig. 7**

**Fig. 8****Fig. 9**

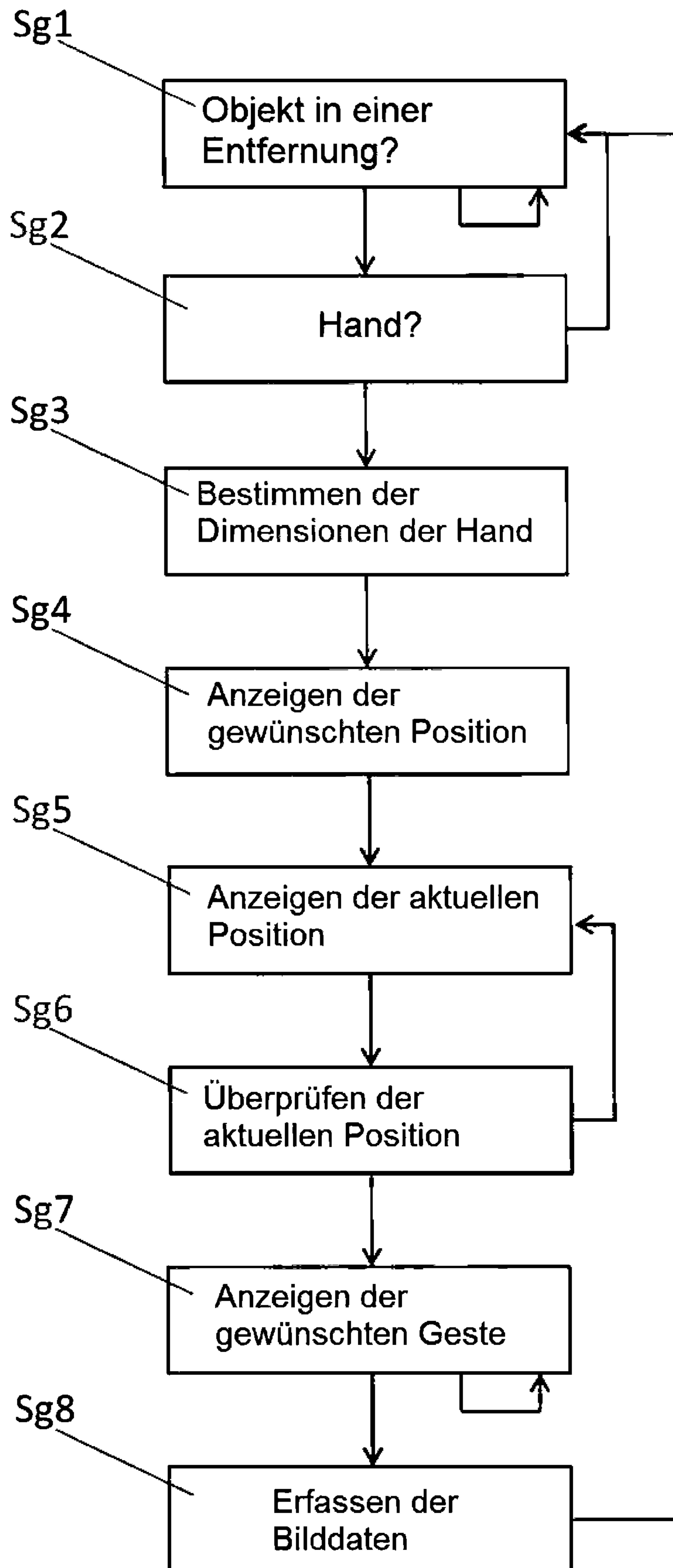


Fig. 10

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS**

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

KENNZEICHNUNG DER NATIONALEN ANMELDUNG	AKTENZEICHEN DES ANMELDERS ODER ANWALTS
	SMAS-010-P-CH
Nationales Aktenzeichen	Anmeldedatum
4832019	10-04-2019
Anmelde-land	Beanspruchtes Prioritätsdatum
CH	
Anmelder (Name)	
Smart Secure ID AG	
Datum des Antrags auf eine Recherche Internationaler Art	Nummer, die die internationale Recherchenbehörde dem Antrag auf eine Recherche internationaler Art zugeteilt hat
19-09-2019	SN74466
I. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDS (treffen mehrere Klassifikationssymbole zu, so sind alle anzugeben)	
Nach der internationalen Patentklassifikation (IPC) oder sowohl nach der nationalen Klassifikation als auch nach der IPC	
G06F21/32; G06K9/00; H04L9/32; H04L29/06	
II. RECHERCHIERTE SACHGEBIETE	
Recherchierter Mindestprüfstoff	
Klassifikationssystem	Klassifikationssymbole
IPC	G06K; G06F; H04L
Recherchierte, nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Sachgebiete fallen	
III. ☐ EINIGE ANSPRÜCHE HABEN SICH ALS NICHT RECHERCHIERBAR ERWIESEN (Bemerkungen auf Ergänzungsbogen)	
IV. ☐ MANGELNDE EINHEITLICHKEIT DER ERFINDUNG (Bemerkungen auf Ergänzungsbogen)	

Formblatt PCT/ISA 201 a (11/2009)

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Nr. des Antrags auf Recherche

CH 4832019

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

INV. G06F21/32 G06K9/00 H04L9/32 H04L29/06
ADD.

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RESEARCHIERTE SACHGEBIETE

Researchierter Mindeststoff (Klassifikationssystem und Klassifikationssymbole)

G06K G06F H04L

Researchierte, aber nicht zum Mindeststoff gehörende Veröffentlichungen, soweit diese unter die researchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE VERÖFFENTLICHUNGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 2 506 188 A2 (FUJITSU LTD [JP]) 3. Oktober 2012 (2012-10-03) * Abbildungen 58, 6, 7, 12B, 13, 19, 20, 21 *	1-15
X	US 2006/018523 A1 (SAITOH HIROFUMI [JP] ET AL) 26. Januar 2006 (2006-01-26)	1, 10
A	* Absatz [0062] - Absatz [0064]; Abbildung 8 *	2-9, 11, 15
A	EP 1 903 509 A1 (FUJITSU LTD [JP]; FUJITSU FRONTTECH LTD [JP]) 26. März 2008 (2008-03-26) * Absatz [0086] - Absatz [0089]; Abbildungen 11, 12 *	1-15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen:

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt wurden soll, oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T spätere Veröffentlichung, die nach dem Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis der der Erfindung zugrundeliegenden Prinzipien oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindungsfähiger Tätigkeit beruhend betrachtet werden

** Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindungsfähiger Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist

Z Veröffentlichung, die Mängel derselben Patentfamilie ist

Datum des tatsächlichen Abschlusses der Recherche internationaler Art

12. November 2019

Abschließendes Datum des Berichts über die Recherche internationaler Art

19.11.2019

Name und Postanschrift der internationalen Recherchenbehörde

Europäischer Patentamt, P.B. 5018 Patentkanal 2
NL - 2280 HW Rijswijk
Tel. (+31-70) 340-2040
Fax: (+31-70) 340-3010

Bevollmächtigter Sachverständiger

Jardak, Christine

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Nr. des Antrags auf Recherche

CH 4832919

Im Recherchenbericht angeführtes Patentsdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung	
EP 2506188	A2	03-10-2012	EP 2506188 A2	03-10-2012
		JP 5810581 B2	11-11-2015	
		JP 2012208682 A	25-10-2012	
		US 2012250954 A1	04-10-2012	

US 2006018523	A1	26-01-2006	KEINE	

EP 1903509	A1	26-03-2008	CN 101145199 A	19-03-2008
		EP 1903509 A1	26-03-2008	
		JP 4786483 B2	05-10-2011	
		JP 2008071158 A	27-03-2008	
		KR 20080025340 A	20-03-2008	
		US 2008226136 A1	18-09-2008	
