(19) Deutsches Patent- und Markenamt

(10) **DE 11 2021 007 504 T5** 2024.02.29

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2022/264331**
in der deutschen Übersetzung (Art. III § 8 Abs. 2 IntPatÜbkG)
(21) Deutsches Aktenzeichen: **11 2021 007 504.7**
(86) PCT-Aktenzeichen: **PCT/JP2021/022916**
(86) PCT-Anmeldetag: **16.06.2021**
(87) PCT-Veröffentlichungstag: **22.12.2022**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **29.02.2024**

(51) Int Cl.: ***G06V 10/70*** (2022.01)
***G06V 10/62*** (2022.01)

(71) Anmelder:
**Mitsubishi Electric Corporation, Tokyo, JP**

(74) Vertreter:
**Pfenning, Meinig & Partner mbB Patentanwälte, 10719 Berlin, DE**

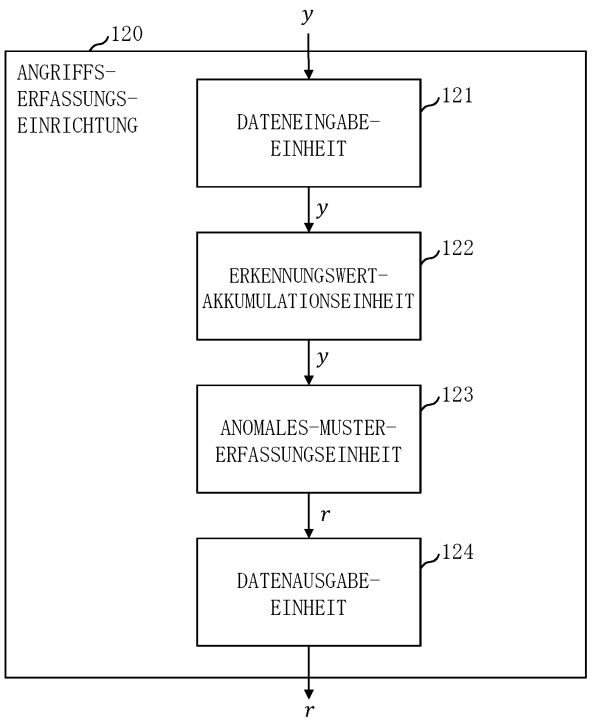
(72) Erfinder:
**Koseki, Yoshihiro, Tokyo, JP**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.**

(54) Bezeichnung: **ANGRIFFSERFASSUNGSEINRICHTUNG, SCHÄDLICHES-SAMPLE-PATCH-ERFASSUNGSSYSTEM, ANGRIFFSERFASSUNGSVERFAHREN UND ANGRIFFSERFASSUNGSPROGRAMM**

(57) Zusammenfassung: Eine Angriffserfassungseinrichtung (120) umfasst eine Anomales-Muster-Erfassungseinheit (123) zum Erfassen, ob ein anomales Muster in einem Zeitreihenerkennungswert enthalten ist, der Zeitreihendaten entspricht, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden, die jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet werden, die in einem Bereich innerhalb eines Bildaufnahmebereichs zu gegenseitig unterschiedlichen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen werden, und entsprechend zum Angeben von Ergebnissen der Erfassung von Objekten in der Vielzahl von Bilddatenteilen. Das anomale Muster ist ein Muster, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist.



## Beschreibung

### TECHNISCHES GEBIET

**[0001]** Die vorliegende Offenbarung bezieht sich auf eine Angriffserfassungseinrichtung, ein Schädliches-Sample-Patch-Erfassungssystem, ein Angriffserfassungsverfahren und ein Angriffserfassungsprogramm.

### HINTERGRUND ZUM STAND DER TECHNIK

**[0002]** In den letzten Jahren wurden bei Aufgaben zur Objekterfassung, bei denen die Position jedes Objekts in einem Eingabebild durch einen Begrenzungsrahmen und die Art jedes Objekts durch ein Label bzw. eine Kennzeichnung angegeben wird, mit Techniken des Deep Learning bzw. tiefen Lernens unter Verwendung neuronaler Netze sehr hohe Genauigkeiten erzielt. In Nicht-Patentliteratur 1 wird eine Technik eines schädlichen Sample-Patch-Angriffs offenbart, bei der die Erfassung durch Objekterfassung umgangen wird, wenn ein schädliches Sample-Patch, das durch Drucken eines Bildes erhalten wird, auf das elektronische Transformationen angewendet wurden, physisch platziert wird und ein aufgenommenes Bild des platzierten schädlichen Sample-Patch eingegeben wird.

### REFERENZLISTE

### NICHT-PATENTLITERATUR

**[0003]** Nicht-Patentliteratur 1: S. Thys et al., „Fooling automated surveillance cameras: adversarial patches to attack person detection“, CVPRW (Conference on Computer Vision and Pattern Recognition Workshops), IEEE (Institute of Electrical and Electronics Engineers) /CVF (Computer Vision Foundation), 2019

### KURZFASSUNG DER ERFINDUNG

### TECHNISCHES PROBLEM

**[0004]** Bei der bestehenden Technik besteht ein Problem darin, dass wenn ein schädlicher Sample-Patch-Angriff ausgeführt wird, der Angriff schwer zu erfassen ist.

**[0005]** Ein Ziel der vorliegenden Offenbarung ist es, einen schädlichen Sample-Patch-Angriff zu erfassen, wenn der Angriff ausgeführt wird.

### LÖSUNG DER AUFGABE

**[0006]** Eine Angriffserfassungseinrichtung gemäß der vorliegenden Offenbarung umfasst
eine Anomales-Muster-Erfassungseinheit zum Erfassen, ob ein anomales Muster in einem Zeitreihenerkennungswert enthalten ist, der Zeitreihendaten entspricht, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden, die jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet werden, die in einem Bereich innerhalb eines Bildaufnahmebereichs zu gegenseitig unterschiedlichen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen werden, wobei die Vielzahl von Erkennungswerten jeweils Ergebnisse der Erfassung von Objekten in der Vielzahl von Bilddatenteilen angeben, wobei das anomale Muster ein Muster ist, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist.

### VORTEILHAFTE WIRKUNGEN DER ERFINDUNG

**[0007]** Eine Angriffserfassungseinrichtung gemäß der vorliegenden Offenbarung umfasst eine Anomales-Muster-Erfassungseinheit, die erfasst, ob ein Zeitreihenerkennungswert, der sich aus Erkennungswerten zusammensetzt, die Ergebnisse der Erfassung von Objekten angeben, ein anomales Muster enthält, das auftritt, wenn ein schädlicher Sample-Patch-Angriff ausgeführt wird. Daher kann der Angriff gemäß der vorliegenden Offenbarung, wenn ein schädlicher Sample-Patch-Angriff ausgeführt wird, erfasst werden.

### KURZBESCHREIBUNG DER ZEICHNUNGEN

**Fig.** 1 ist eine Darstellung, die ein Beispiel für eine Systemkonfiguration eines Schädliches-Sample-Patch-Erfassungssystems 100 gemäß Ausführungsform 1 zeigt;

**Fig.** 2 ist eine Darstellung, die ein Beispiel für eine funktionale Konfiguration einer Objekterfassungseinrichtung 110 gemäß Ausführungsform 1 zeigt;

**Fig.** 3 ist eine Darstellung, die ein Beispiel für eine funktionale Konfiguration einer Angriffserfassungseinrichtung 120 gemäß Ausführungsform 1 zeigt;

**Fig.** 4 ist eine Darstellung, die ein Beispiel für eine Hardware-Konfiguration jeder der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 gemäß Ausführungsform 1 zeigt;

**Fig.** 5 ist ein Ablaufdiagramm, das eine Funktionsweise des Schädliches-Sample-Patch-Erfassungssystems 100 gemäß Ausführungsform 1 zeigt; und

**Fig.** 6 ist eine Darstellung, die ein Beispiel für die Hardware-Konfiguration jeder der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 gemäß einer Variante von Ausführungsform 1 zeigt.

## BESCHREIBUNG DER AUSFÜHRUNGSFORMEN

**[0008]** In der Beschreibung und den Zeichnungen der Ausführungsformen sind die gleichen Elemente und entsprechende Elemente mit dem gleichen Bezugszeichen benannt. Die Beschreibung von Elementen, die mit dem gleichen Bezugszeichen benannt sind, wird gegebenenfalls weggelassen oder vereinfacht. Pfeile in Darstellungen zeigen hauptsächlich Daten- oder Verarbeitungsflüsse an. „Einheit“ kann gegebenenfalls als „Schaltung“, „Schritt“, „Vorgang“, „Prozess“ oder „Schaltkreis“ interpretiert werden.

### Ausführungsform 1.

**[0009]** Diese Ausführungsform wird nachstehend unter Bezugnahme auf die Zeichnungen beschrieben.

#### *** Beschreibung der Konfiguration ***

**[0010] Fig.** 1 zeigt ein Beispiel für eine Systemkonfiguration eines Schädliches-Sample-Patch-Erfassungssystems 100 gemäß dieser Ausführungsform. Das Schädliches-Sample-Patch-Erfassungssystem 100 umfasst eine Objekterfassungseinrichtung 110 und eine Angriffserfassungseinrichtung 120. Die Objekterfassungseinrichtung 110 und die Angriffserfassungseinrichtung 120 können als Einheit eingerichtet werden.

**[0011]** Die Objekterfassungseinrichtung 110 empfängt Eingabebilddaten x als Eingabe und gibt einen Erkennungswert y aus, der ein Ergebnis der Objekterfassung ist.

**[0012]** Die Angriffserfassungseinrichtung 120 empfängt den Erkennungswert y als Eingabe und gibt als Erfassungsergebnis r eines schädlichen Sample-Patch-Angriffs ein Ergebnis aus, das angibt, dass ein schädlicher Sample-Patch-Angriff erfasst worden ist, wenn ein anomales Muster eines Erkennungswerts aufgrund eines schädlichen Sample-Patch-Angriffs erfasst wird, und ein Ergebnis, das angibt, dass in anderen Fällen kein schädlicher Sample-Patch-Angriff erfasst worden ist. Ein schädlicher Sample-Patch-Angriff ist eine Art von schädlichem Sample-Angriff und ist insbesondere ein Angriff, der die Objekterfassung durch ein neuronales Netz oder ähnliches umgeht. Ein anomales Muster ist beispielsweise ein Muster, bei dem der Wert eines Erkennungswerts über eine bestimmte Zeitperiode hinweg leicht unter einem Objekterfassungsschwellenwert liegt. Das heißt, dass das anomale Muster ein Muster ist, das angibt, dass eine Zeitperiode, in der der Wert eines Erkennungswertes, der durch einen Zeitreihenerkennungswert angegeben wird, geringer als der Objekterfassungsschwellenwert ist und gleich wie oder größer als ein Anomalieerfassungsschwellenwert ist, für eine Anomalieerfassungszeitperiode oder länger andauert. Ein Angriff mit einem vorhandenen schädlichen Sample-Patch kann den Wert eines Erkennungswerts unter den Objekterfassungsschwellenwert senken, kann den Wert aber nicht vollständig auf 0 setzen. Daher ist dieses anomale Muster zum Erfassen des Angriffs geeignet. Das anomale Muster ist jedoch nicht auf dieses Muster beschränkt.

**[0013] Fig.** 2 veranschaulicht ein Beispiel einer funktionalen Konfiguration der Objekterfassungseinrichtung 110. Die Objekterfassungseinrichtung 110 umfasst eine Dateneingabeeinheit 111, einen Objekterfasser 112 und eine Datenausgabeeinheit 113.

**[0014]** Die Dateneingabeeinheit 111 empfängt Eingabebilddaten x, die ein Ziel einer Objekterfassung sind, und gibt die empfangenen Eingabebilddaten x an den Objekterfasser 112 ein.

**[0015]** Der Objekterfasser 112 berechnet einen Erkennungswert y unter Verwendung der eingegebenen Eingabebilddaten x und gibt den berechneten Erkennungswert y an die Datenausgabeeinheit 113 aus. Bei dem Objekterfasser 112 handelt es sich beispielsweise um den mit einem neuronalen Netz aufgebauten Objekterfasser 112. Bei dem neuronalen Netz handelt es sich beispielsweise um You Only Look Once (YOLO), Single Shot Multibox Detector (SSD), Faster region-based convolutional neural networks (R-CNN) oder ähnliches. Der Objekterfasser 112 gibt als Erkennungswert Koordinaten aus, die die Position eines Begrenzungsrahmens darstellen, der jedem im Eingabebild erscheinenden Objekt entspricht, sowie einen Typ und eine Wahrscheinlichkeit, die einen Vertrauensgrad für das Objekt in jedem Begrenzungsrahmen angibt. Der Objekterfasser 112 berechnet eine Vielzahl von Erkennungswerten unter Verwendung einer Vielzahl von Bilddatenteilen. Der Objekterfasser 112 wird auch als Objekterfassungseinheit bezeichnet.

**[0016]** Die Datenausgabeeinheit 113 gibt den vom Objekterfasser 112 berechneten Erkennungswert y aus.

**[0017] Fig.** 3 zeigt ein Beispiel für eine funktionale Konfiguration der Angriffserfassungseinrichtung 120. Die Angriffserfassungseinrichtung 120 umfasst eine Dateneingabeeinheit 121, eine Erkennungswertakkumulationseinheit 122, eine Anomales-Muster-Erfassungseinheit 123 und eine Datenausgabeeinheit 124.

**[0018]** Die Dateneingabeeinheit 121 empfängt den Erkennungswert y und gibt den empfangenen Erkennungswert y an die Erkennungswertakkumulationseinheit 122 ein.

**[0019]** Die Erkennungswertakkumulationseinheit 122 addiert den eingegebenen Erkennungswert y zu einem Zeitreihenerkennungswert Y', um einen Zeitreihenerkennungswert Y zu erzeugen, und gibt den erzeugten Zeitreihenerkennungswert Y in die Anomales-Muster-Erfassungseinheit 123 ein. Der Zeitreihenerkennungswert Y entspricht dem Zeitreihenerkennungswert Y', der aktualisiert wurde. Der Zeitreihenerkennungswert Y' entspricht Zeitreihendaten, die durch Akkumulieren der Erkennungswerte y erzeugt werden, die vor der Eingabe eines neuen Erkennungswertes y eingegeben wurden. Die Erkennungswertakkumulationseinheit 122 muss nicht jedes Mal, wenn der Erkennungswert y in die Erkennungswertakkumulationseinheit 122 eingegeben wird, den Zeitreihenerkennungswert Y in die Anomales-Muster-Erfassungseinheit 123 eingeben, und die Anomales-Muster-Erfassungseinheit 123 kann den letzten Zeitreihenerkennungswert Y in regelmäßigen Abständen von der Erkennungswertakkumulationseinheit 122 abrufen und den abgerufenen Zeitreihenerkennungswert Y verwenden. Ein Zeitreihenerkennungswert entspricht Zeitreihendaten, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden. Die Vielzahl von Erkennungswerten werden jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet, die von einem Bereich innerhalb eines Bildaufnahmebereichs zu voneinander verschiedenen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen wurden, und geben Ergebnisse der jeweiligen Erfassung von Objekten in der Vielzahl von Bilddatenteilen an.

**[0020]** Die Anomales-Muster-Erfassungseinheit 123 prüft, ob der Zeitreihenerkennungswert Y mit einem im Voraus spezifizierten anomalen Muster übereinstimmt. Die Anomales-Muster-Erfassungseinheit 123 gibt in die Datenausgabeeinheit 124 als Erfassungsergebnis r ein Ergebnis ein, das die Erfassung angibt, wenn der Zeitreihenerkennungswert Y mit dem anomalen Muster übereinstimmt, oder ein Ergebnis, das angibt, dass kein schädlicher Sample-Patch-Angriff erfasst wurde, wenn der Zeitreihenerkennungswert Y nicht mit dem anomalen Muster übereinstimmt. Die Anomales-Muster-Erfassungseinheit 123 bestimmt, dass ein Angriff mit einem schädlichen Sample-Patch durchgeführt wurde, wenn das anomale Muster, bei dem es sich um einen Übergang handelt, der sich von einem Übergang der Erkennungswerte zu normalen Zeiten unterscheidet, erfasst wird. Die Anomales-Muster-Erfassungseinheit 123 erfasst, ob das anomale Muster, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist, in dem Zeitreihenerkennungswert enthalten ist.

**[0021]** Die Datenausgabeeinheit 124 gibt das eingegebene Erfassungsergebnis r aus.

**[0022]** **Fig.** 4 ist eine Darstellung, die ein Beispiel für Hardware-Ressourcen jeder der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 gemäß dieser Ausführungsform zeigt. Jede der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 wird durch einen Computer gebildet oder kann durch eine Vielzahl von Computern gebildet werden.

**[0023]** Jede der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 umfasst einen Prozessor 11. Der Prozessor 11 ist über einen Bus 12 mit Hardware-Einrichtungen wie einem ROM 13, einem RAM 14, einer Kommunikationsplatine 15, einer Anzeige 51, die eine Anzeigeeinrichtung ist, einer Tastatur 52, einer Maus 53, einem Laufwerk 54 und einer Magnetplatteneinrichtung 20 verbunden und steuert diese Hardware-Einrichtungen. Der Prozessor 11 ist eine integrierte Schaltung (IC: integrated circuit), die eine Betriebsverarbeitung durchführt, und ist als konkretes Beispiel eine zentrale Verarbeitungseinheit (CPU: central processing unit), ein Digitalsignalprozessor (DSP: digital signal processor) oder eine Grafikverarbeitungseinheit (GPU: graphics processing unit). Jede der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 kann eine Vielzahl von Prozessoren umfassen. Die Vielzahl von Prozessoren teilen sich die Rolle des Prozessors 11.

**[0024]** Das Laufwerk 54 ist eine Einrichtung, die von einem Speichermedium wie einem Flexible Disk Drive (FD), einer Compact Disc (CD) und einer Digital Versatile Disc (DVD) liest und darauf schreibt.

**[0025]** Der ROM 13, der RAM 14, die Magnetplatteneinrichtung 20 und das Laufwerk 54 sind jeweils ein Beispiel für eine Speichereinrichtung. Die Speichereinrichtung kann unabhängig von dem Computer sein.

**[0026]** Die Tastatur 52, die Maus 53 und die Kommunikationsplatine 15 sind jeweils ein Beispiel für eine Eingabeeinrichtung. Die Anzeige 51 und die Kommunikationsplatine 15 sind jeweils ein Beispiel für eine Ausgabeeinrichtung.

**[0027]** Die Kommunikationsplatine 15 ist drahtgebunden oder drahtlos mit einem Kommunikationsnetz wie einem lokalen Netzwerk (LAN), dem Internet oder einer Telefonleitung verbunden. In einem konkreten Beispiel besteht die Kommunikationsplatine 15 aus einem Kommunikationschip oder einer Netzwerkschnittstellenkarte (NIC).

**[0028]** Die Magnetplatteneinrichtung 20 speichert ein Betriebssystem (OS) 21, Programme 22 und Dateien 23.

**[0029]** Die Programme 22 umfassen Programme, die Funktionen ausführen, die in dieser Ausführungsform als jede Einheit oder jede Einrichtung beschrieben werden. Die Programme werden von dem Prozessor 11 gelesen und ausgeführt. Das heißt, die Programme veranlassen einen Computer, als jede Einheit oder jede Einrichtung zu arbeiten, oder veranlassen einen Computer, Vorgänge oder Verfahren jeder Einheit oder jeder Einrichtung durchzuführen.

**[0030]** Jedes beliebige in dieser Spezifikation erläuterte Programm kann in einem computerlesbaren nicht-flüchtigen Aufzeichnungsmedium aufgezeichnet sein. Das nicht-flüchtige Aufzeichnungsmedium ist, als ein konkretes Beispiel, eine optische Scheibe oder ein Flash-Speicher. Jedes in dieser Spezifikation beschriebene Programm kann als ein Programmprodukt bereitgestellt sein.

**[0031]** Die Dateien 23 enthalten verschiedene Arten von Daten, die in jeder Einheit oder jeder Einrichtung, die in dieser Ausführungsform beschrieben werden, verwendet werden.

*** Beschreibung einer Funktionsweise ***

**[0032]** Ein Funktionsvorgang der Objekterfassungseinrichtung 110 entspricht einem Objekterfassungsverfahren. Ein Programm, das die Funktion der Objekterfassungseinrichtung 110 realisiert, entspricht einem Objekterfassungsprogramm. Ein Funktionsvorgang der Angriffserfassungseinrichtung 120 entspricht einem Angriffserfassungsverfahren. Ein Programm, das die Funktion der Angriffserfassungseinrichtung 120 realisiert, entspricht einem Angriffserfassungsprogramm.

**[0033]** **Fig.** 5 ist ein Ablaufdiagramm, das eine Beispielverarbeitung des Schädliches-Sample-Patch-Erfassungssystems 100 gemäß dieser Ausführungsform zeigt. Anhand dieser Darstellung wird die Verarbeitung des Schädliches-Sample-Patch-Erfassungssystems 100 beschrieben.

(Schritt S11)

**[0034]** Die Dateneingabeeinheit 111 empfängt Eingabebilddaten x und gibt die empfangenen Eingabebilddaten x an den Objekterfasser 112 ein.

(Schritt S12)

**[0035]** Der Objekterfasser 112 berechnet einen Erkennungswert y unter Verwendung der eingegebenen Eingabebilddaten x.

(Schritt S13)

**[0036]** Die Datenausgabeeinheit 113 gibt den berechneten Erkennungswert y aus.

(Schritt S14)

**[0037]** Die Dateneingabeeinheit 121 empfängt den Erkennungswert y und gibt den empfangenen Erkennungswert y an die Erkennungswertakkumulationseinheit 122 ein.

(Schritt S15)

**[0038]** Die Erkennungswertakkumulationseinheit 122 addiert den eingegebenen Erkennungswert y zu einem Zeitreihenerkennungswert Y', um den Zeitreihenerkennungswert Y' zu einen Zeitreihenerkennungswert Y zu aktualisieren, und gibt den aktualisierten Zeitreihenerkennungswert Y in die Anomales-Muster-Erfassungseinheit 123 ein.

(Schritt S16)

**[0039]** Die Anomales-Muster-Erfassungseinheit 123 bestimmt, ob der eingegebene Zeitreihenerkennungswert Y mit einem im Voraus spezifizierten anomalen Muster übereinstimmt.

**[0040]** Wenn das anomale Muster mit dem Zeitreihenerkennungswert Y übereinstimmt, geht die Angriffserfassungseinrichtung 120 zu Schritt S17 über. In anderen Fällen geht die Angriffserfassungseinrichtung 120 zu Schritt S18 über.

(Schritt S17)

**[0041]** Die Datenausgabeeinheit 124 gibt als Erfassungsergebnis r ein Ergebnis aus, das angibt, dass ein schädlicher Sample-Patch-Angriff erfasst wurde.

(Schritt S18)

**[0042]** Die Datenausgabeeinheit 124 gibt als Erfassungsergebnis r ein Ergebnis aus, das angibt, dass kein schädlicher Sample-Patch-Angriff erfasst wurde.

*** Beschreibung der Wirkungen von Ausführungsform 1 ***

**[0043]** Wie oben beschrieben, kann ein schädlicher Sample-Patch-Angriff gemäß dieser Ausführungsform dadurch erfasst werden, dass bestimmt wird, ob ein Zeitreihenerkennungswert mit einem anomalen Muster übereinstimmt.

*** Andere Konfigurationen ***

<Variante 1>

**[0044]** **Fig.** 6 zeigt ein Beispiel für die Hardware-Konfiguration jeder der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 gemäß dieser Variante.

**[0045]** Die Objekterfassungseinrichtung 110 und die Angriffserfassungseinrichtung 120 enthalten jeweils eine Verarbeitungsschaltung 18 anstelle des Prozessors 11, anstelle des Prozessors 11 und des ROM 13, anstelle des Prozessors 11 und des RAM 14 oder anstelle des Prozessors 11, des ROM 13 und des RAM 14.

**[0046]** Bei der Verarbeitungsschaltung 18 handelt es sich um eine Hardware, die zumindest einen Teil der in der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 enthaltenen Einheiten realisiert.

**[0047]** Die Verarbeitungsschaltung 18 kann dedizierte Hardware sein oder kann ein Prozessor sein, der Programme ausführt, die in der Magnetplatteneinrichtung 20 gespeichert sind.

**[0048]** Wenn es sich bei der Verarbeitungsschaltung 18 um dedizierte Hardware handelt, ist ein konkretes Beispiel für die Verarbeitungsschaltung 18 eine einzelne Schaltung, eine zusammengesetzte Schaltung, ein programmierter Prozessor, ein parallel-programmierter Prozessor, eine anwendungsspezifische integrierte Schaltung (ASIC), ein feldprogrammierbares Gate Array (FPGA) oder eine Kombination davon.

**[0049]** Jede der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 kann eine Vielzahl von Verarbeitungsschaltungen als Alternative zu der Verarbeitungsschaltung 18 umfassen. Die Vielzahl von Verarbeitungsschaltungen teilen sich die Rolle der Verarbeitungsschaltung 18.

**[0050]** In der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 können jeweils einige Funktionen durch spezielle Hardware und die übrigen Funktionen durch Software oder Firmware realisiert werden.

**[0051]** In einem konkreten Beispiel wird die Verarbeitungsschaltung 18 durch Hardware, Software, Firmware oder eine Kombination daraus realisiert.

**[0052]** Der Prozessor 11, der ROM 13, der RAM 14 und die Verarbeitungsschaltung 18 werden zusammen als „Verarbeitungsschaltkreis“ bezeichnet. Das heißt, die Funktionen der funktionalen Komponenten jeder der Objekterfassungseinrichtung 110 und der Angriffserfassungseinrichtung 120 sind durch den Verarbeitungsschaltkreis realisiert.

*** Weitere Ausführungsformen ***

**[0053]** Ausführungsform 1 wurde beschrieben und Teile dieser Ausführungsform können in Kombination implementiert sein. Alternativ kann diese Ausführungsform teilweise implementiert werden. Alternativ kann diese Ausführungsform auf verschiedene Arten nach Bedarf modifiziert werden und kann ganz oder teilweise in beliebiger Kombination implementiert sein. Was als jede Einheit oder jede Einrichtung beschrieben ist, kann durch Firmware, Software, Hardware oder eine Kombination davon implementiert werden.

**[0054]** Die vorstehend beschriebene Ausführungsform ist ein im Wesentlichen bevorzugtes Beispiel und ist nicht dazu bestimmt, die vorliegende Offenbarung sowie die Anwendungen und den Umfang von Einsatzbereichen der vorliegenden Offenbarung einzuschränken. Die in den Ablaufdiagrammen oder dergleichen beschriebenen Vorgänge können nach Bedarf geändert werden.

BEZUGSZEICHENLISTE

**[0055]** 11: Prozessor, 12: Bus, 13: ROM, 14: RAM, 15: Kommunikationsplatine, 18: Verarbeitungsschaltung, 20: Magnetplatteneinrichtung, 21: OS, 22: Programme, 23: Dateien, 51: Anzeige, 52: Tastatur, 53: Maus, 54: Laufwerk, 100: Schädliches-Sample-Patch-Erfassungssystem, 110: Objekterfassungseinrichtung, 111: Dateneingabeeinheit, 112: Objekterfasser, 113: Datenausgabeeinheit, 120: Angriffserfassungseinrichtung, 121: Dateneingabeeinheit, 122: Erkennungswertakkumulationseinheit, 123: Anomales-Muster-Erfassungseinheit, 124: Datenausgabeeinheit.

**Patentansprüche**

1. Angriffserfassungseinrichtung, umfassend eine Anomales-Muster-Erfassungseinheit zum Erfassen, ob ein anomales Muster in einem Zeitreihenerkennungswert enthalten ist, der Zeitreihendaten entspricht, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden, die jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet werden, die in einem Bereich innerhalb eines Bildaufnahmebereichs zu gegenseitig unterschiedlichen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen werden, wobei die Vielzahl von Erkennungswerten jeweils Ergebnisse der Erfassung von Objekten in der Vielzahl von Bilddatenteilen angeben, wobei das anomale Muster ein Muster ist, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist.

2. Angriffserfassungseinrichtung nach Anspruch 1, wobei das anomale Muster ein Muster ist, das angibt, dass eine Zeitperiode, in der ein Wert eines Erkennungswertes, der durch den Zeitreihenerkennungswert angegeben wird, geringer als ein Objekterfassungsschwellenwert und gleich wie oder größer als ein Anomalieerfassungsschwellenwert ist,

für eine Anomalieerfassungszeitperiode oder länger andauert.

3. Schädliches-Sample-Patch-Erfassungssystem, umfassend:
die Angriffserfassungseinrichtung nach Anspruch 1 oder 2; und
eine Objekterfassungseinrichtung mit einer Objekterfassungseinheit, die die Vielzahl von Erkennungswerten jeweils unter Verwendung der Vielzahl von Bilddatenteilen berechnet.

4. Angriffserfassungsverfahren, umfassend Erfassen, ob ein anomales Muster in einem Zeitreihenerkennungswert enthalten ist, der Zeitreihendaten entspricht, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden, die jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet werden, die in einem Bereich innerhalb eines Bildaufnahmebereichs zu gegenseitig unterschiedlichen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen werden, wobei die Vielzahl von Erkennungswerten jeweils Ergebnisse der Erfassung von Objekten in der Vielzahl von Bilddatenteilen angeben, wobei das anomale Muster ein Muster ist, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist.

5. Angriffserfassungsprogramm, das eine Angriffserfassungseinrichtung, die ein Computer ist, veranlasst, auszuführen einen Anomales-Muster-Erfassungsprozess des Erfassens, ob ein anomales Muster in einem Zeitreihenerkennungswert enthalten ist, der Zeitreihendaten entspricht, die unter Verwendung einer Vielzahl von Erkennungswerten erzeugt werden, die jeweils unter Verwendung einer Vielzahl von Bilddatenteilen berechnet werden, die in einem Bereich innerhalb eines Bildaufnahmebereichs zu gegenseitig unterschiedlichen Zeitpunkten innerhalb eines Bildaufnahmezeitbereichs aufgenommen werden, wobei die Vielzahl von Erkennungswerten jeweils Ergebnisse der Erfassung von Objekten in der Vielzahl von Bilddatenteilen angeben, wobei das anomale Muster ein Muster ist, das auftritt, wenn ein schädlicher Sample-Patch-Angriff gegen mindestens eines der Vielzahl von Bilddatenteilen durchgeführt worden ist.

Es folgen 6 Seiten Zeichnungen

**Anhängende Zeichnungen**

Fig. 1

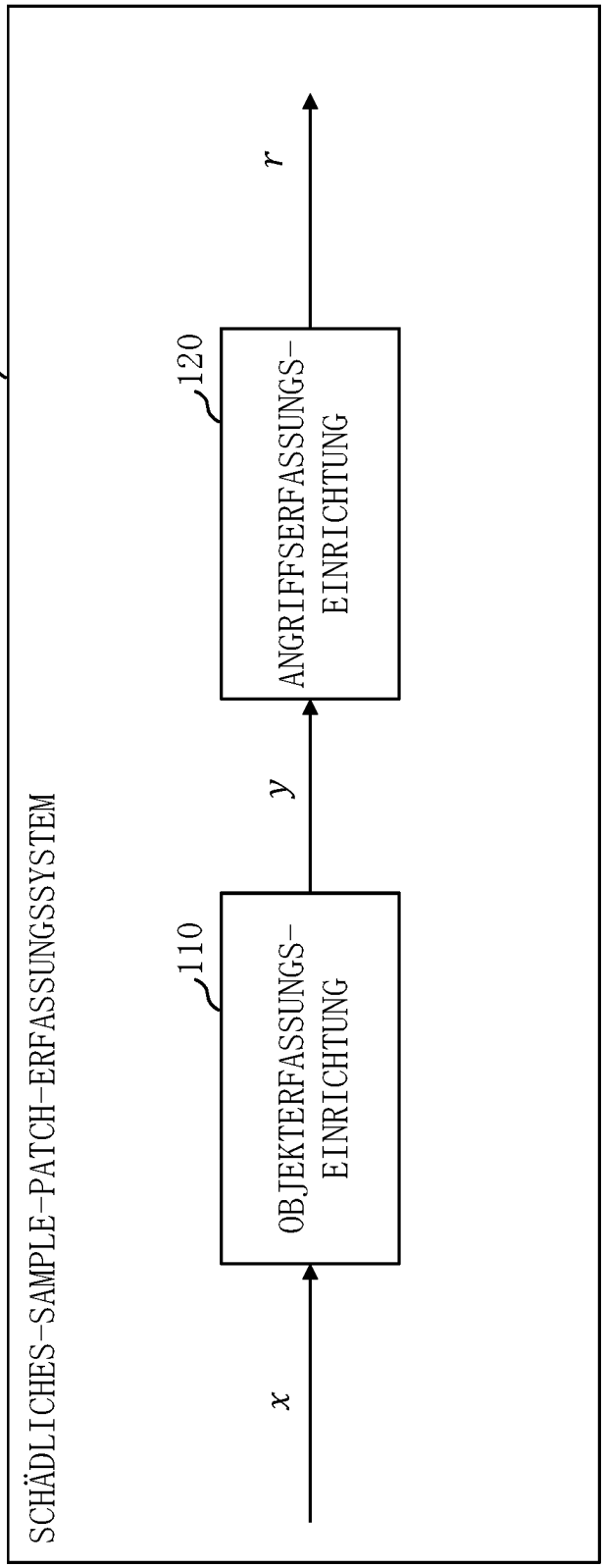


Fig. 2

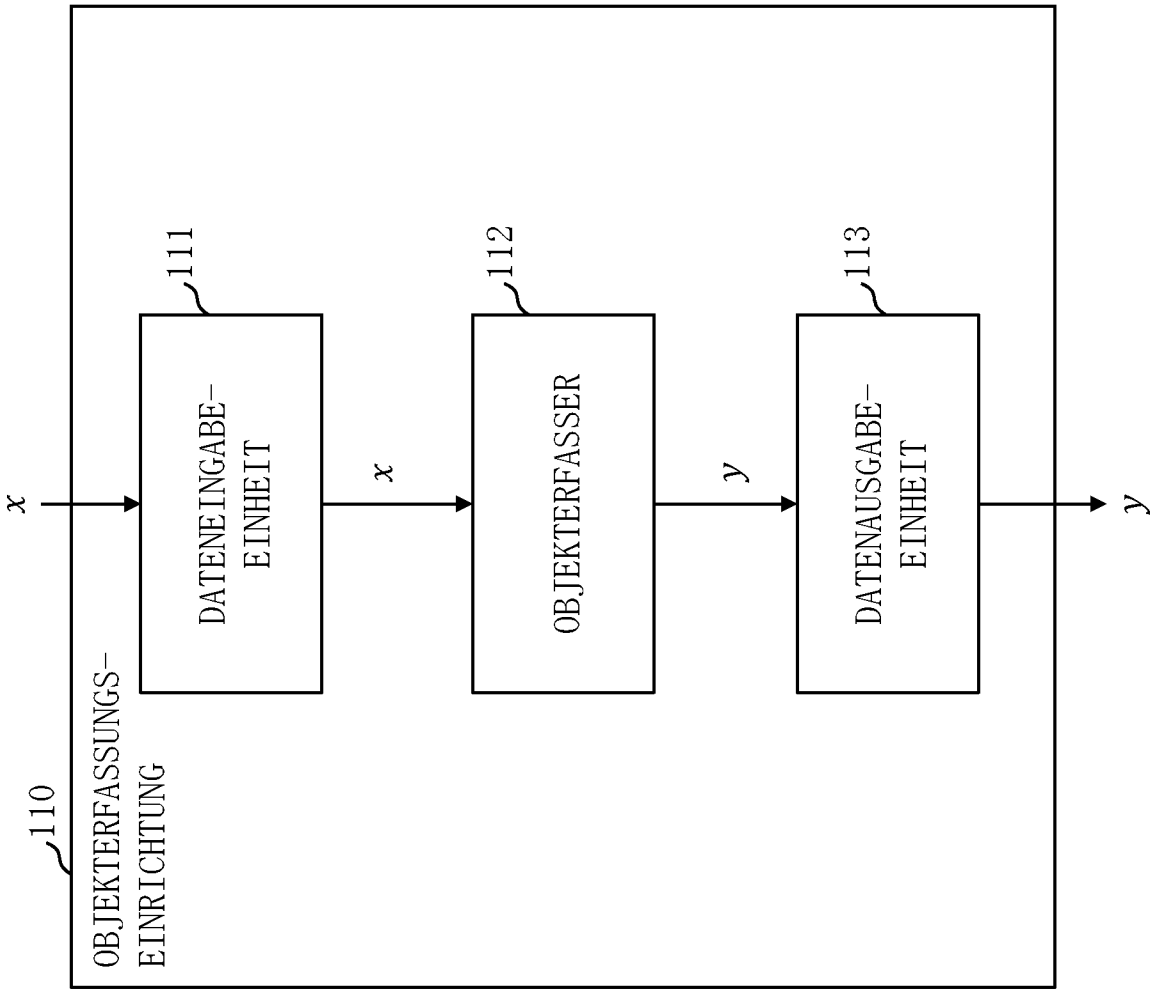

110
OBJEKTERFASSUNGS-
EINRICHTUNG
111
DATENEINGABE-
EINHEIT
112
OBJEKTERFASSER
113
DATENAUSGABE-
EINHEIT
x
x
y
y

Fig. 3

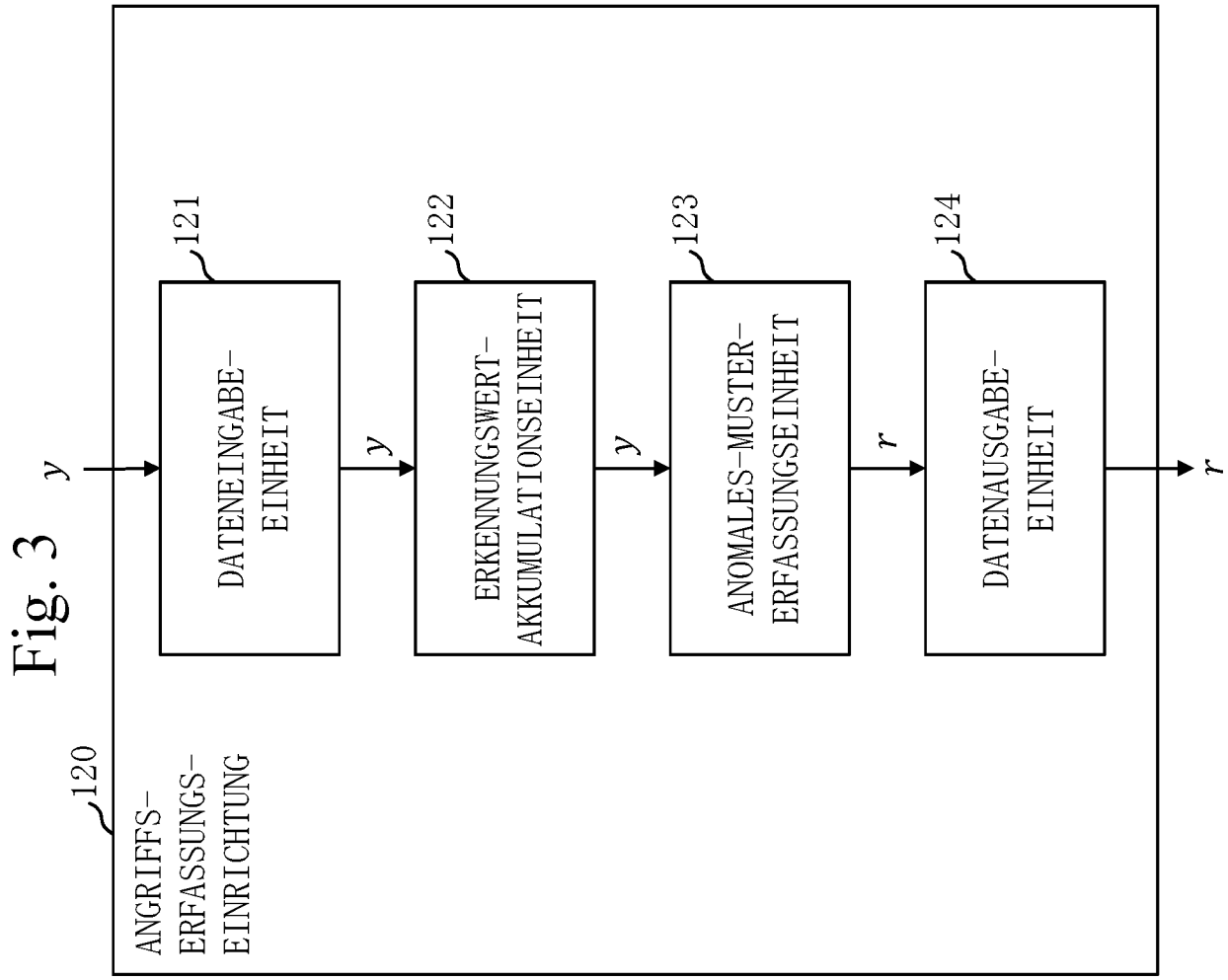

120
ANGRIFFS-ERFASSUNGS-EINRICHTUNG
y
121
DATENEINGABE-EINHEIT
y
122
ERKENNUNGSWERT-AKKUMULATIONSEINHEIT
y
123
ANOMALES-MUSTER-ERFASSUNGSEINHEIT
r
124
DATENAUSGABE-EINHEIT
r

Fig. 4

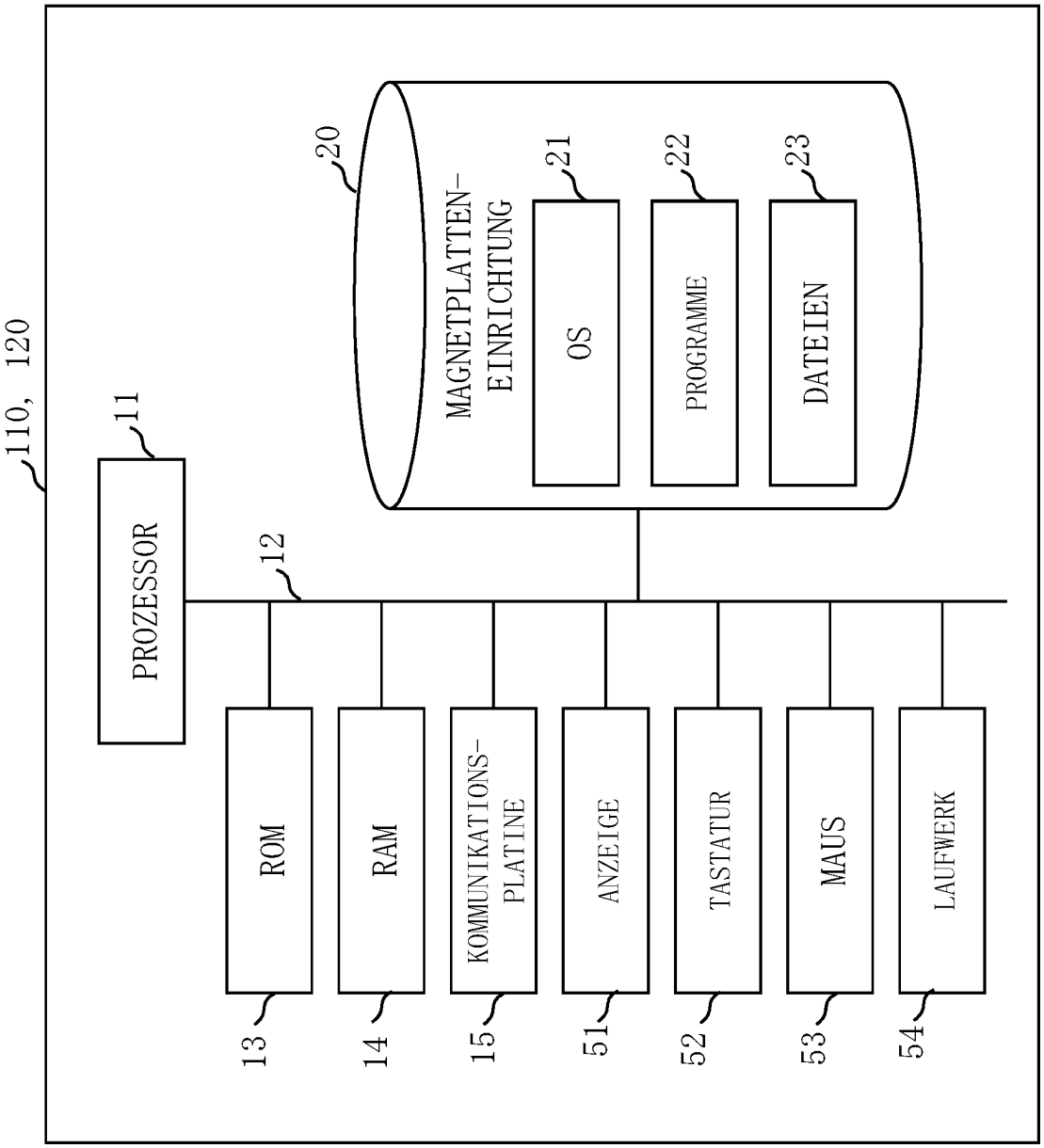

110, 120
PROZESSOR
11
12
20
MAGNETPLATTEN-EINRICHTUNG
21
OS
22
PROGRAMME
23
DATEIEN
ROM
13
RAM
14
KOMMUNIKATIONS-PLATINE
15
ANZEIGE
51
TASTATUR
52
MAUS
53
LAUFWERK
54

Fig. 5

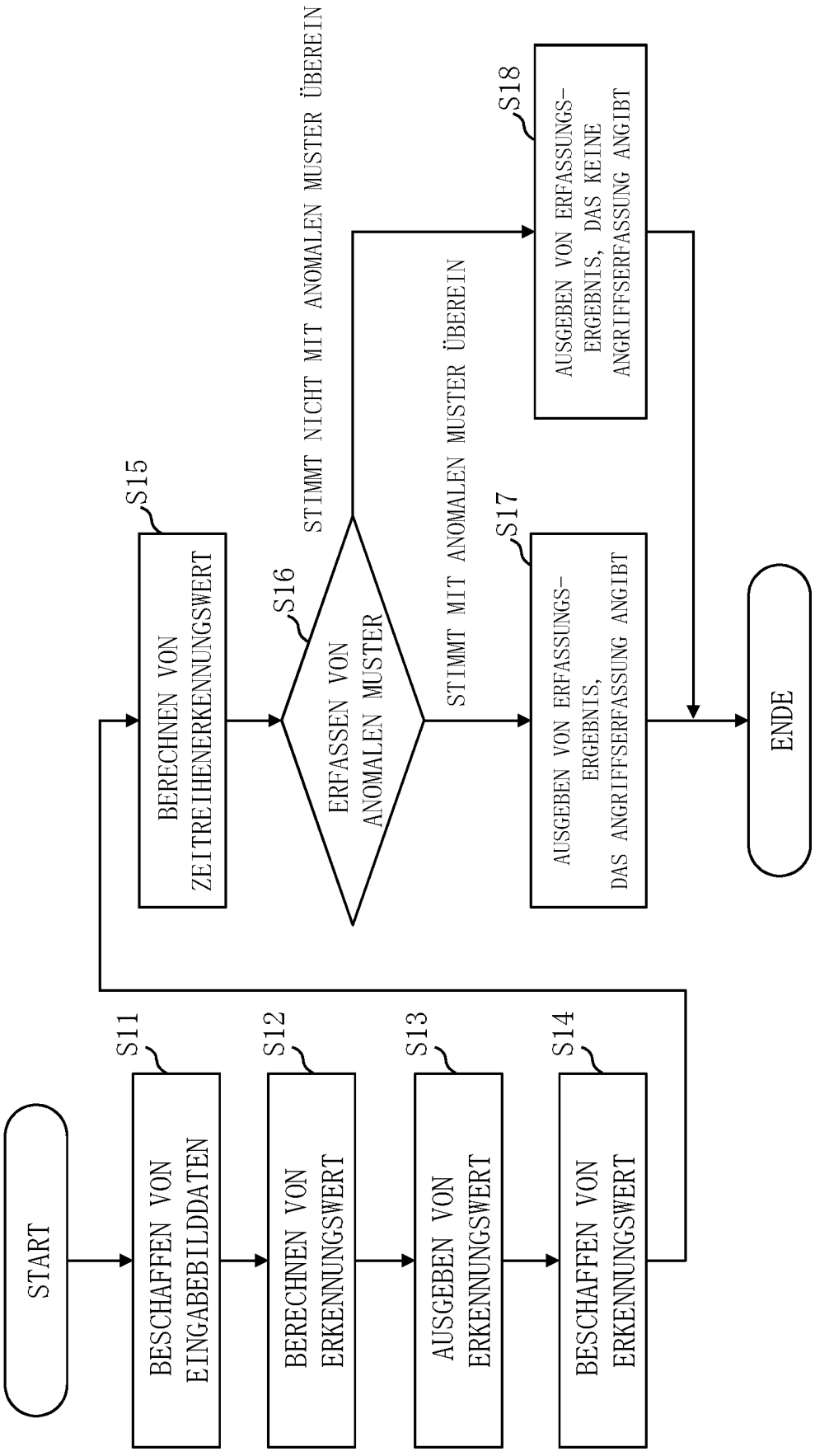
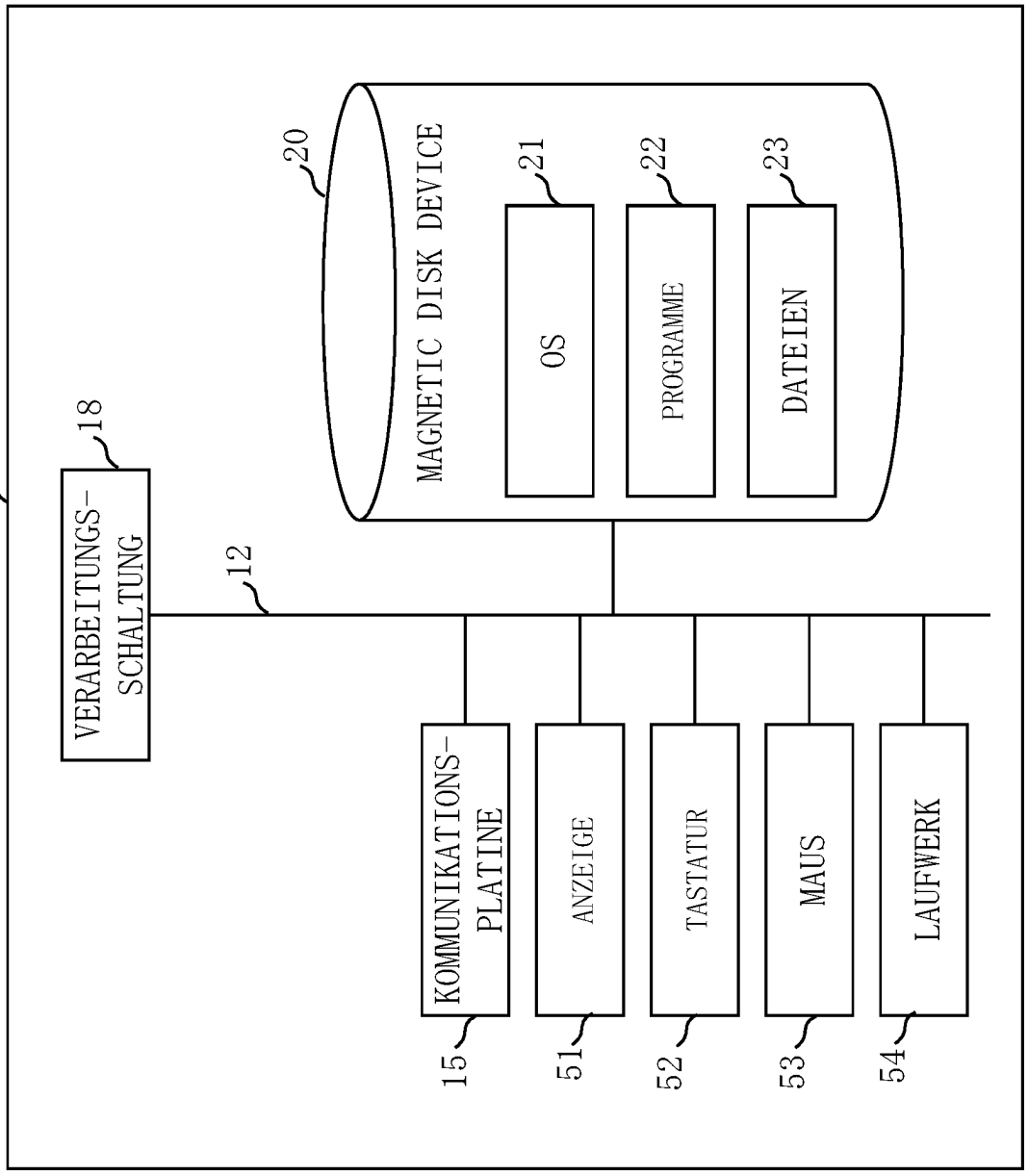

START
S11
BESCHAFFEN VON EINGABEBILDDATEN
S12
BERECHNEN VON ERKENNUNGSWERT
S13
AUSGEBEN VON ERKENNUNGSWERT
S14
BESCHAFFEN VON ERKENNUNGSWERT
S15
BERECHNEN VON ZEITREIHENERKENNUNGSWERT
S16
ERFASSEN VON ANOMALEN MUSTER
STIMMT MIT ANOMALEN MUSTER ÜBEREIN
STIMMT NICHT MIT ANOMALEN MUSTER ÜBEREIN
S17
AUSGEBEN VON ERFASSUNGS-ERGEBNIS, DAS ANGRIFFSERFASSUNG ANGIBT
S18
AUSGEBEN VON ERFASSUNGS-ERGEBNIS, DAS KEINE ANGRIFFSERFASSUNG ANGIBT
ENDE

Fig. 6




 Das Dokument wurde durch die Firma Luminess hergestellt.