(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2004 024 002 A1** 2005.12.01

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2004 024 002.7**
(22) Anmeldetag: **14.05.2004**
(43) Offenlegungstag: **01.12.2005**

(51) Int Cl.[7]: **G01D 21/00**
G01D 4/08, H04L 9/32, G07C 11/00

(71) Anmelder:
AEG Infrarot-Module GmbH, 74072 Heilbronn, DE

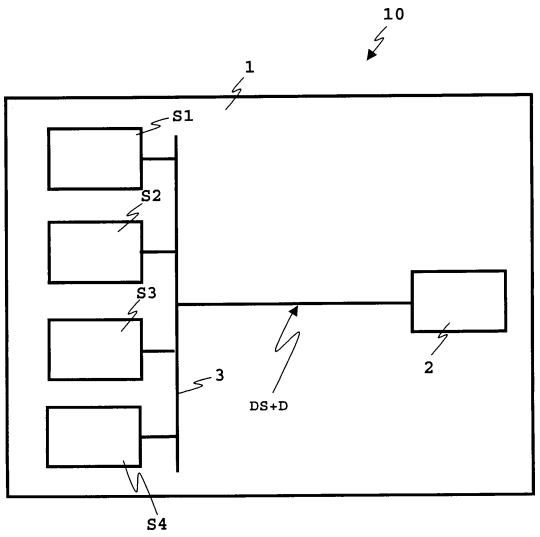
(72) Erfinder:
Eberhardt, Kurt, 89081 Ulm, DE; Stifter, Peter, Dr., 89195 Staig, DE; Hofmann, Karl, Dr., 89081 Ulm, DE; Erni, Arnold, 88400 Biberach, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Authentifizierung von Sensordaten und zugehörigem Sensor**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Authentifizierung von Sensordaten (D), die zwischen mindestens einem Sensor (S1 bis S4) und einem zugehörigen Empfänger (2) ausgetauscht werden, bei dem zunächst vom Empfänger (2) eine Anforderung (Challenge) an den mindestens einen Sensor (S1 bis S4) mit einer verschlüsselten Zufallszahl übertragen wird, diese Anforderung von dem mindestens einen Sensor (S1 bis S4) entschlüsselt, die Zufallszahl modifiziert und die modifizierte Zufallszahl als Einmalschlüssel (Session-Key, Sitzungsschlüssel) für die nachfolgende Sensordatenübertragung (Response) verwendet wird, indem sensorseitig ein erster Hashwert (H) aus den Sensordaten (D) berechnet; eine kryptographische Prüfsumme (DS) zur Authentifizierung der zu übertragenden Sensordaten (D) erzeugt wird, indem aus dem ersten Hashwert (H) und dem Einmalschlüssel als Datenblock ein zweiter Hashwert (H') errechnet und mit dem geheimen Sensorschlüssel (GS) verschlüsselt wird, die authentifizierten Sensordaten (DS+D) an den Empfänger (2) übertragen wird, und empfängerseitig die kryptographische Prüfsumme (DS) auf Authentizität überprüft wird.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Authentifizierung von Sensordaten und einen zugehörigen Sensor.

Stand der Technik

[0002] Im Bereich von Sicherheitsanwendungen sind Sensoren zur Überwachung von Gegenständen und Gebäuden sowie bei der Identifizierung von Personen üblich. Viele Eindringversuche und Attacken finden statt, um diese Systeme zu täuschen und zu überwinden. Bei derzeitigen Systemen ist eine Schnittstelle zwischen dem Sensor und einem zugehörigen Empfänger in der Regel als ungesicherte Datenschnittstelle ausgeführt. Der Grund dafür ist, dass bildgebende Sensoren eine große zu übertragende Datenmenge erzeugen, deren Verschlüsselung eine erhebliche Rechenleistung erfordert. So dauert z.B. bei der Übertragung von Videodaten die Verschlüsselung der Videodaten länger als eine Sekunde und erfordert eine erhebliche Rechenleistung bei einer softwarebasierten Realisierung. Eine Integration eines für diese Rechenleistung erforderlichen Mikrocontrollers ist im Sensor technisch nur schwer realisierbar.

[0003] Aus der Offenlegungsschrift DE 199 63 329 A1 ist ein Sensormodul mit einer Authentifizierungseinheit bekannt, das zu übertragende Sensordaten mit kryptographischen Verfahren sichert. Zur Sicherung der zu übertragenden Sensordaten wird beispielsweise ein Hashwert berechnet und mit einem geheimen Sensorschlüssel (GS) verschlüsselt, mit dem die zu übertragenden Sensordaten authentifiziert werden.

[0004] Kryptographische Hash-Funktionen sind mathematische Methoden, die aus einem beliebigen Datenstrom (z. Bsp. Sensordaten, Klartext) nach einem vorbestimmten Verfahren einen Wert vorgegebener Länge im Sinne einer Prüfsumme (Hashwert) erzeugen bzw. berechnen. Hash-Funktionen dienen vornehmlich dazu, die Unverfälschtheit (Integrität) von Daten und Texten nachzuweisen.

[0005] Gemäß der oben genannten DE 199 63 329 A1 wird im Empfänger der verschlüsselte Hashwert entschlüsselt und überprüft. Dadurch kann der Ursprung und die Unversehrtheit der Sensordaten sichergestellt werden. Bei den vom Sensormodul erfassten Daten handelt es sich vorzugsweise um Verbrauchsdaten, beispielsweise von Gas-, Strom-, Wasserzählern usw. oder um biometrische Merkmalsdaten, beispielsweise Fingerlinien, die einen wesentlich kleineren Datenumfang als bild-gebende Sensoren aufweisen.

[0006] Aufgabe der Erfindung ist es, ein Verfahren zur Authentifizierung von Sensordaten für eine manipulationssichere Datenübertragung anzugeben sowie einen zugehörigen Sensor zur Verfügung zu stellen.

[0007] Die Erfindung löst diese Aufgabe durch Bereitstellung eines Verfahrens zur Authentifizierung von Sensordaten mit den Merkmalen des Patentanspruchs 1 und durch einen Sensor mit den Merkmalen des Patentanspruchs 5. Vorteilhafte Verwendungen des Sensors werden durch die Patentansprüche 8 und 9 beansprucht.

[0008] Vorteilhafte Ausführungsformen und Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen angegeben.

[0009] Erfindungsgemäß wird zur Authentisierung der Sensordaten die Berechnung einer kryptographischen Prüfsumme mit einem Challenge-Response-Verfahren (Anforderungs-Antwort-Verfahren) verknüpft, wobei diese kryptographische Prüfsumme als Authentisierungsdaten im Anschluss an die Sensordaten an den Empfänger übermittelt wird. Damit können in vorteilhafter Weise im Empfänger die übertragenen Daten in Echtzeit verarbeitet und unmittelbar nach der Überprüfung für gültig oder ungültig erklärt werden.

[0010] Zur Durchführung dieses Challenge-Response-Verfahren wird zwischen dem mindestens einen Sensor und dem Empfänger ein Session-Key (Sitzungs-schlüssel bzw. Einmalschlüssel) erzeugt. Hierzu empfängt der mindestens eine Sensor vom Empfänger eine Anforderung (Challenge) mit einer verschlüsselten Zufallszahl, die der mindestens eine Sensor entschlüsselt und diese nach einem auf beiden Seiten bekannten Verfahren modifiziert. Diese modifizierte Zufallszahl wird dann als Datenblock verschlüsselt an den Empfänger zurückgeschickt und stellt die Antwort (Response) zu dessen Anforderung dar. Der Empfänger, dem neben dem Session-Key auch der geheime Sensorschlüssel (GS) bekannt ist, empfängt diesen Datenblock, führt dieselbe Modifikation wie der Sensor an seiner Originalzufallszahl durch und vergleicht beide Zahlenwerte. Bei einer Übereinstimmung der Zahlenwerte ist die Authentizität des Sensors in Bezug auf den Empfänger in dieser Übertragungssession abgesichert. Ein solcher Session-Key ist nur für eine kurze Zeit, also nur für eine Session oder eine angeforderte Datenübertragung gültig.

[0011] Ein weiterer Vorteil des erfindungsgemäßen Verfahrens wird durch die Einbeziehung der zu übertragenden Sensordaten in die Bildung der kryptographischen Prüfsumme für die Authentifizierung der Sensordaten erzielt, da dadurch die Überprüfung der Unversehrtheit der übertragenen Daten möglich ist. Denn eine Manipulation der Sensordaten hätte eine

veränderte Prüfsumme zur Folge hat, die bei der Auswertung durch den Empfänger erkannt würde. Durch das erfindungsgemäße Verfahren wird auch bei öffentlicher Kenntnis eine durchgängige Sicherheitskette vom Sensor, der die Daten erfasst, bis zu einer zentralen Datenverwaltung mit gesicherter Infrastruktur ermöglicht, wodurch eine unerkannte Manipulation der übertragenen Sensordaten nahezu unmöglich wird.

[0012] Zur Hashwertberechnung, also zur Bildung der kryptographischen Prüfsumme werden etablierte Standardverfahren verwendet.

[0013] Gemäß einer vorteilhaften Weiterbildung der Erfindung erfolgt parallel zur seriellen Übertragung der Sensordaten die Hashwertberechnung, weshalb dieser Hashwert als kryptographische Prüfsumme in vorteilhafter Weise direkt nach der Übertragung der Sensordaten zur Verfügung steht und damit einfach an die übertragenen Sensordaten angehängt werden kann, mit der Folge, dass für die Verschlüsselung nur wenig Zeit erforderlich ist und damit das gesamte Verfahren beschleunigt wird.

[0014] Um das erfindungsgemäße Verfahren weiter zu beschleunigen, sind nicht alle Sensordaten zur Hashwertberechnung erforderlich, sondern es können eine vorgegebene Anzahl von Sensordaten verwendet werden, bspw. nur jedes dritte Byte. Allerdings wird dadurch die Sicherheit des Verfahrens in Abhängigkeit des Umfanges der verwendeten Sensordaten reduziert.

[0015] Die Überprüfung der empfangenen kryptographischen Prüfsumme erfolgt in dem Empfänger, indem zunächst aus den empfangenen Sensordaten ein Hashwert berechnet wird, und zwar nach dem gleichen Verfahren, mit dem im Sensor der Zweite Hashwert erzeugt wird, anschließend die kryptographische Prüfsumme entschlüsselt und schließlich das Entschlüsselungsergebnis mit dem zuerst aus dem empfangenen Sensordaten errechneten Hashwert auf Identität verglichen wird.

[0016] Ein erfindungsgemäßer Sensor umfasst Mittel zum Erzeugen von Sensordaten, eine Authentifizierungseinheit, die ihrerseits einen Prüfsummengenerator zur Erzeugung der kryptographischen Prüfsumme und eine Verschlüsselungseinheit zur Verschlüsselung des letzten, also des zweiten Hashwertes umfasst. Der Sensor ist beispielsweise als bildgebender Sensor, vorzugsweise als Infrarotkamera und/oder Digitalkamera, ausgeführt.

[0017] In Ausgestaltung des erfindungsgemäßen Sensors ist die Authentifizierungseinheit auf dem Sensorbaustein (Sensorchip) integriert und erfordert zur Implementierung des erfindungsgemäßen Verfahrens nur ca. 10% zusätzliche Chipfläche. Dadurch ist trotz verbessertem Manipulationsschutz eine kompakte Ausführungsform des Sensors möglich.

[0018] Bei einer Weiterbildung ist der erfindungsgemäße Sensor Teil eines Personenidentifikationssystems.

[0019] Bei einer anderen Weiterbildung ist der erfindungsgemäße Sensor Teil eines Überwachungssystems für Gegenstände und/oder Gebäude.

Ausführungsbeispiel

[0020] Eine vorteilhafte Ausführungsform der Erfindung ist in den Zeichnungen dargestellt und wird nachfolgend beschrieben.

[0021] Dabei zeigen:

[0022] Fig. 1 ein schematisches Blockschaltbild eines Überwachungssystems, und

[0023] Fig. 2 ein Blockschaltbild eines Sensors des Überwachungssystems aus Fig. 1.

[0024] Wie aus Fig. 1 ersichtlich ist, umfasst ein Überwachungssystem **10**, beispielsweise für ein Gebäude **1**, mehrere Sensoren S1 bis S4, die über ein Bussystem **3** mit einem Empfänger **2** verbunden sind, der beispielsweise Teil einer zentralen Datenverwaltung ist, in der die mit einer kryptographischen Prüfsumme DS übertragenen Sensordaten D ausgewertet und verarbeitet werden. Die beispielhaft dargestellten Sensoren S1 bis S4 sind vorzugsweise als bildgebende Sensoren, beispielsweise als Infrarot- und/oder Digitalkamera ausgeführt. Im Bereich von Sicherheitsanwendungen werden solche bildgebenden Sensoren S1 bis S4 zur Überwachung von Gegenständen und Gebäuden sowie bei der Identifizierung von Personen benutzt. Es finden viele Eindringversuche und Attacken statt, um diese Systeme zu täuschen, zu manipulieren und zu überwinden. Deshalb müssen solche Täuschungs- und/oder Manipulationsversuche erkannt und im Empfänger **2** ein entsprechender Alarm ausgelöst werden. Daher wird im dargestellten Überwachungssystem **10** das erfindungsgemäße Verfahren zur Authentifikation von Sensordaten D angewendet, das nachfolgend im Zusammenhang mit Fig. 2 beschrieben wird.

[0025] Fig. 2 zeigt ein detailliertes Blockschaltbild des Sensors S1 aus Fig. 1, wobei nur für die Erfindung relevante Komponenten dargestellt sind. Wie aus Fig. 2 ersichtlich ist, umfasst der bildgebende Sensor S1 Bildaufnahmemittel **5**, eine Datenverarbeitungseinrichtung **6**, eine Authentifizierungseinheit **4** mit einem Prüfsummengenerator **4.1** und einer Verschlüsselungseinheit **4.2** und eine Ausgabesteuerschaltung **7**.

[0026] Die Bildaufnahmemittel **5** umfassen beispielsweise Infrarotsensoren und/oder optische Sensoren, die Bildinformationen eines überwachten Umfeldes aufnehmen und als Sensordaten D zur weiteren Verarbeitung und Auswertung zur Verfügung stellen. In der Datenverarbeitungseinheit **6** werden die von den Bildaufnahmemitteln **5** zur Verfügung gestellten Sensordaten D zur Durchführung einer Blockchiffrierung blockweise, also als Datenblöcke D_i von jeweils gleicher Länge in den Prüfsummengenerator **4.1** eingelesen.

[0027] Zur Authentifizierung der Sensordaten wird die Berechnung einer kryptographischen Prüfsumme DS mit einem Challenge-Response-Verfahren (Anforderungs-Antwort-Verfahren) verknüpft, wobei diese kryptographische Prüfsumme DS als Authentisierungsdaten im Anschluss an die Sensordaten an den Empfänger übermittelt wird. Hierzu wird zur Erzeugung eines Session-Key (Sitzungs-schlüssel bzw. Einmalschlüssel) vom Empfänger **2** eine Anforderung (Challenge) an den Sensor S1 gesendet, die eine verschlüsselte Zufallszahl enthält und von dem Sensor S1 dekryptiert und nach einem auf beiden Seiten bekannten Verfahren modifiziert wird.

[0028] Diese modifizierte Zufallszahl wird dann als Datenblock verschlüsselt an den Empfänger zurückgeschickt und stellt die Antwort (Response) zu dessen Anforderung dar. Der Empfänger, dem neben dem Session-Key auch der geheime Sensorschlüssel GS bekannt ist, empfängt diese kryptographische Prüfsumme DS, führt dieselbe Modifikation wie der Sensor an seiner Originalzufallszahl durch und vergleicht beide Zahlenwerte. Bei einer Übereinstimmung der Zahlenwerte ist die Authentizität des Sensors in Bezug auf den Empfänger in dieser Übertragungssession abgesichert. Ein solcher Session-Key ist nur für eine kurze Zeit, also nur für eine Session oder eine angeforderte Datenübertragung gültig.

[0029] Zur Berechnung der kryptographischen Prüfsumme DS wird mittels des Prüfsummengenerator **4.1** zuerst ein erster Hashwert H für die Gesamtheit aller zu übertragenden Daten bestimmt und anschließend mit der Verschlüsselungseinheit **4.2** verschlüsselt.

[0030] Zur Hashwertberechnung kann jedes etablierte Standardverfahren verwendet werden. Beispielhaft soll jedoch im folgenden ein Verfahren zur Hashwertberechnung dargestellt und beschrieben werden. Bei diesem mittels eines Blockchiffrierers durchgeführten Verfahrens wird der erste Hashwert H mittels eines Iterationsverfahrens aus Hashwerten H_i, i = 0, 1, ... N erzeugt, wobei parallel zur Übertragung der Sensordaten aus jedem i-ten Datenblock der in Datenblöcken D_i aufgeteilten Sensordaten mittels des in der vorangegangenen (i – 1)-ten Iteration erzeugten Hashwertes ein Hashwert der i-ten Iteration berechnet wird.

[0031] Mittels des Prüfsummengenerators **4.1** wird der i-te Hashwert H_i aus dem i-ten Datenblock errechnet, indem dieser mit dem Hashwert H_{i-1} als Schlüssel verschlüsselt wird.

[0032] Als Startwert H_0 zur Berechnung des ersten Hashwertes H_1 für den ersten Datenblock D_1 wird ein geheimer in der Verschlüsselungseinheit **4.2** gespeicherter Sensorschlüssel GS und/oder ein aus dem Sensorschlüssel abgeleiteter Wert verwendet.

[0033] Der letzte iterativ erzeugt Hashwert H_N wird als Schlüssel mit dem Session-Key (Sitzungsschlüssel, Einmalschlüssel) als Datenblock nochmals einer Hashwertberechnung zur Erzeugung des zweiten Hashwertes H' unterzogen. Der resultierende Hashwert H' wird der Verschlüsselungseinheit **4.2** zugeführt und dort mit dem geheimen Sensorschlüssel GS zur Bildung der kryptographischen Prüfsumme DS verschlüsselt. Die kryptographische Prüfsumme DS wird als Authentifizierungsdaten mit den Sensordaten D zum Empfänger **2** übermittelt. Damit wird diese kryptographische Prüfsumme DS direkt nach vollständiger Übertragung eines Datenframes auf derselben Schnittstelle, also über die Datenverarbeitungseinrichtung **6** als DS+D an den Empfänger **2** übermittelt.

[0034] Die Ausgabesteuerschaltung **7** überträgt die Sensordaten als Datenframe über entsprechende Kommunikationskanäle, die im dargestellten Ausführungsbeispiel als Datenbus **3** ausgeführt sind, an den Empfänger **2**, wobei am Ende der als Datengruppe (Datenframe) zusammengefasste Sensordaten D die kryptographische Prüfsumme DS angehängt wird, so dass alle Datengruppen der Sensoren mit jeweils der zugehörigen Prüfsumme DS zum Empfänger **2** übertragen werden.

[0035] Der Empfänger **2** kann durch eine hard- oder softwarebasierte Berechnung der kryptographische Prüfsumme DS die Authentizität der empfangenen Daten D überprüfen, da ihm der Schlüssel des sendenden Sensors S1 und der Session-Key bekannt sind.

[0036] Damit wird zunächst aus den empfangenen Sensordaten D ein Hashwert H'_E berechnet, wobei hierzu das gleiche Verfahren angewendet wird, mit dem der Sensor den zweiten Hashwert erzeugt. Anschließend wird die kryptographische Prüfsumme DS entschlüsselt und das Entschlüsselungsergebnis mit dem zuerst aus den empfangenen Sensordaten errechneten Hashwert auf Identität verglichen.

[0037] Daten D von nicht zertifizierten Sensoren oder ohne Authentifizierungsdatei, d.h. ohne Prüfsumme werden verworfen. Wird bei der Überprüfung

der Prüfsumme DS ein Täuschungs- und/oder Manipulationsversuch erkannt, dann löst der Empfänger **2** einen entsprechenden Alarm aus. Zur Übertragung der Daten D können beliebige Kommunikationskanäle, also auch drahtlose Übertragungsverfahren benutzt werden.

[0038] Zur Bildung eines aktuellen Schlüssels für die nachfolgende Datenübertragung werden natürlich für alle Sensoren S1, S2, S3 und S4 mit dem bereits oben beschriebenen Challenge-Response-Verfahren entsprechende Einmalschlüssel (Session-Key) erzeugt, die als aktuelle Schlüssel ausschließlich für die nachfolgende Sensordatenübertragung zwischen dem jeweiligen Sensor und dem Empfänger **2** dienen.

[0039] Durch die Anwendung des erfindungsgemäßen Verfahrens kann die Authentifizierungseinheit **4** auf dem Sensorchip integriert werden, da nur ein zusätzlicher Flächenbedarf von ca. 10% erforderlich ist. Somit können die dargestellten Sensoren S1 bis S4 jeweils als Einchipbaugruppen ausgeführt sein, bei denen alle in Fig. 2 dargestellten Komponenten auf einem einzigen Chip integriert sind. Dieses Verfahren kann auch für eine sichere Datenübertragung bei monolithisch integrierten Sensoren verwendet werden, die in sicherheitsrelevanten Systemen zum Einsatz kommen, beispielsweise Zugangskontrollen, Grenzkontrollen, e-commerce etc., in denen optische und/oder elektrische Sensoren eingesetzt werden, die ein großes Datenaufkommen haben.

[0040] Im dargestellten Ausführungsbeispiel ist der erfindungsgemäße Sensor Teil eines Überwachungssystems für Gegenstände und/oder Gebäude. Selbstverständlich sind auch andere Anwendungen möglich, beispielsweise in einem Personenidentifikationssystem.

[0041] Durch die erfindungsgemäße Einbeziehung der zu übertragenden Sensordaten in die Bildung des Hashwertes für die Authentifizierung der Sensordaten, wird die Überprüfung der Unversehrtheit der übertragenen Daten gewährleistet, da eine Manipulation der Sensordaten eine veränderte Prüfsumme zur Folge hat, die bei der Auswertung durch den Empfänger erkannt wird. Somit eignet sich das erfindungsgemäße Verfahren auch für bildgebende Sensorsysteme in ungeschützter öffentlicher Umgebung mit der Anforderung der sicheren Datenübertragung.

Patentansprüche

1. Verfahren zur Authentifizierung von Sensordaten (D), die zwischen mindestens einem Sensor (S1 bis S4) und einem zugehörigen Empfänger (**2**) ausgetauscht werden, bei dem zunächst vom Empfänger (**2**) eine Anforderung (Challenge) an den mindestens einen Sensor (S1 bis S4) mit einer verschlüsselten Zufallszahl übertragen wird, diese Anforderung von dem mindestens einen Sensor (S1 bis S4) entschlüsselt, die Zufallszahl modifiziert und die modifizierte Zufallszahl als Einmalschlüssel (Session-Key, Sitzungsschlüssel) für die nachfolgende Sensordatenübertragung (Response) gemäß folgenden Schritten verwendet wird:
(1) Sensorseitiges Berechnen eines ersten Hashwertes (H) aus den Sensordaten (D),
(2) Erzeugung einer kryptographischen Prüfsumme (DS) zur Authentifizierung der zu übertragenden Sensordaten (D), indem
a) aus dem ersten Hashwert (H) und dem Einmalschlüssel als Datenblock ein zweiter Hashwert (H') errechnet wird,
b) der zur Bildung der Prüfsumme (DS) zweite Hashwert H' mit einem geheimen Sensorschlüssel (GS) verschlüsselt wird
(3) Übertragen der authentifizierten Sensordaten (DS+D) an den Empfänger (**2**), und
(4) empfängerseitiges Überprüfen der empfangenen kryptographischen Prüfsumme (DS) auf Authentizität.

2. Verfahren nach Anspruch 1, bei dem die Erzeugung des ersten Hashwertes (H) parallel zur seriellen Übertragung der Sensordaten erfolgt.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem nur eine vorgegebene Anzahl der Sensordaten (D) zur Erzeugung des ersten Hashwertes (H) verwendet werden.

4. Verfahren nach einem der vorangehenden Ansprüche, bei dem zur Überprüfung der empfangenen kryptographischen Prüfsumme (DS) auf Authentizität folgende Schritte durchgeführt werden:
a) Empfängerseitiges Berechnen einen Hashwertes (H'_E) aus den empfangenen Sensordaten (D) mit dem im Sensor verwendeten Verfahren zur Berechnung des zweiten Hashwertes (H'),
b) Entschlüsseln der empfangenen kryptographischen Prüfsumme (DS), und
c) Vergleich des Entschlüsselungsergebnisses (H') mit dem Hashwert (H'_E) auf Identität.

5. Sensor zur Durchführung des Authentifizierungsverfahrens nach einem der Ansprüche 1 bis 4 mit
– Mitteln (**5**) zum Erzeugen von Sensordaten (D),
– einer Authentifizierungseinheit (**4**), und
– in der Authentifizierungseinheit (**4**) angeordneten Prüfsummengenerator (**4.1**) zur Erzeugung der kryptographischen Prüfsumme (DS) und einer Verschlüsselungseinheit (**4.2**) zur Verschlüsselung des zweiten Hashwertes (H').

6. Sensor nach Anspruch 5, der als bildgebender Sensor (S1 bis S4), vorzugsweise als Infrarotkamera und/oder Digitalkamera, ausgeführt ist.

7. Sensor nach Anspruch 5 oder 6, dessen Authentifizierungseinheit (**4**) auf einem Sensorbaustein integriert ist.

8. Personenidentifikationssystem mit mindestens einen Sensor (S1 bis S4) nach einem der Ansprüche 6 bis 7.

9. Überwachungssystem für Gegenstände und/oder Gebäude, mit mindestens einen Sensor (S1 bis S4) nach einem der Ansprüche 6 bis 7.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

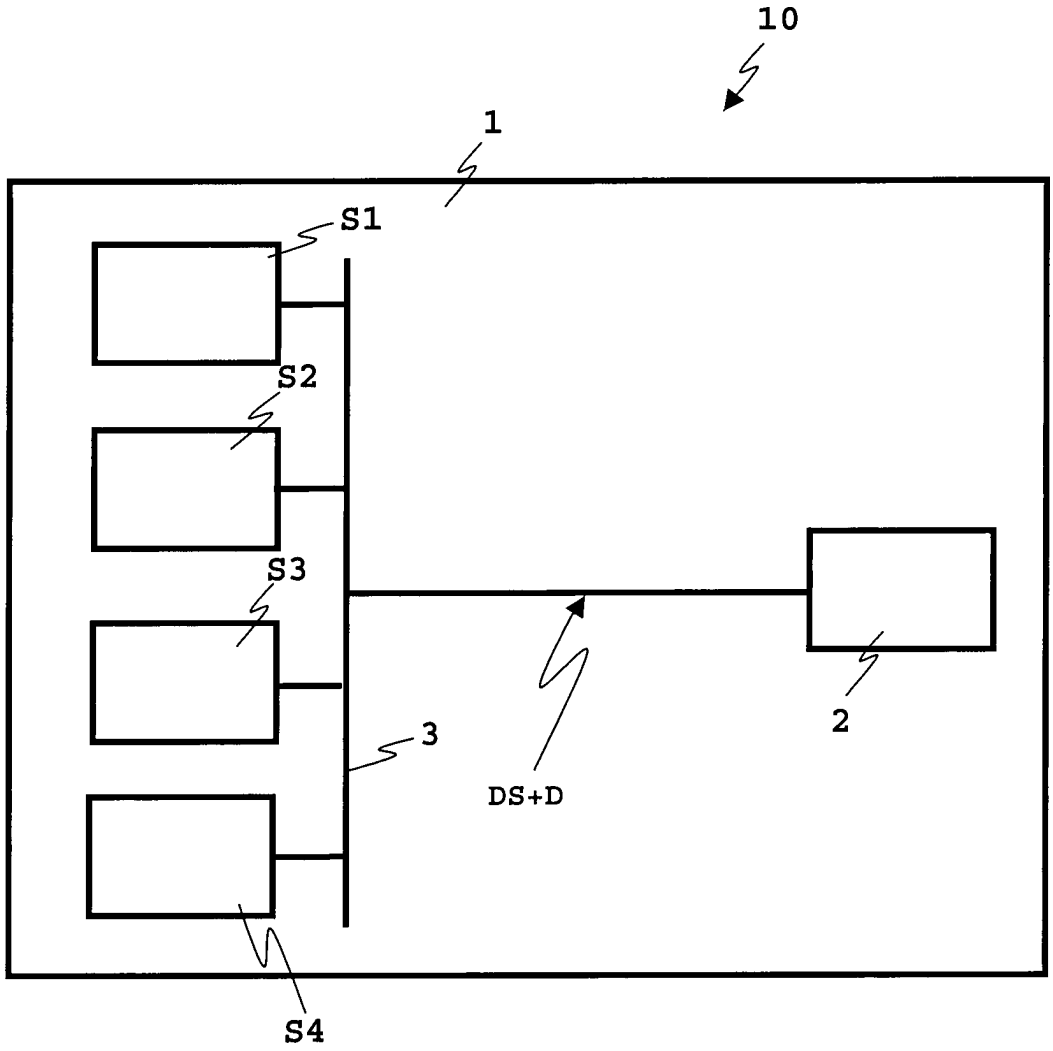


Fig. 1

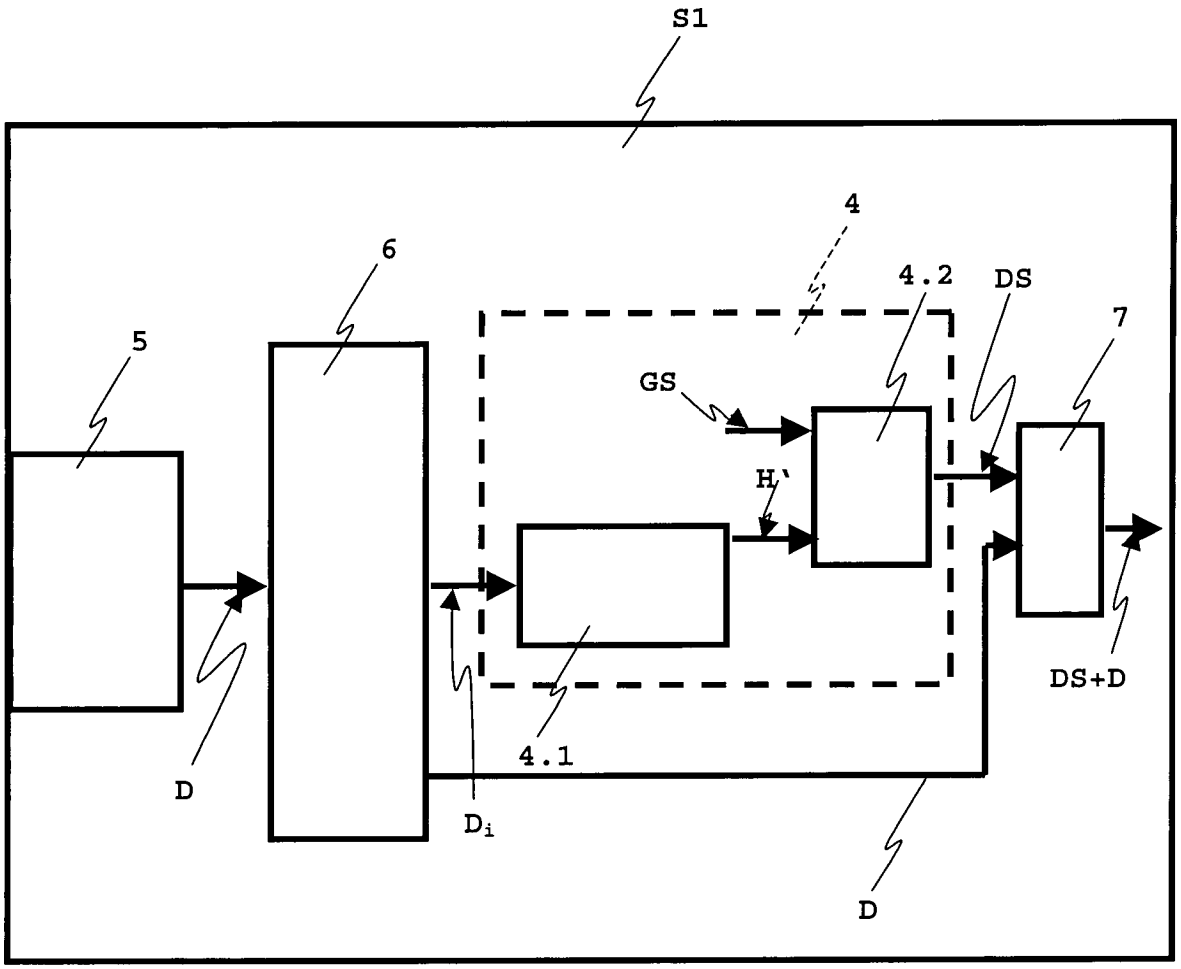


Fig. 2