

(19)
(12)

(KR)
(A)

(51) 。 Int. Cl. ⁷
A61B 5/00

(11)
(43)

2002 - 0064292
2002 08 07

| | |
|------|---------------------|
| (21) | 10 - 2002 - 7004038 |
| (22) | 2002 03 28 |
| | 2002 03 28 |
| (86) | PCT/US2000/27017 |
| (86) | 2000 09 28 |

(87) WO 2001/22873
(87) 2001 04 05

[illegible]

| | | | |
|------|------------|------------|------|
| (30) | 60/156,488 | 1999 09 28 | (US) |
| | 09/662,246 | 2000 09 14 | (US) |

(71) 675(:63042)

(72)

, , .
 94301 764
 ,
 94087 # - 155400
 , , .
 94040 1613
 , , .
 94506 가 4119
 , , .
 94563 61
 ,
 66085 16301

(74)

:

(54)

가

4

가

(pulse oximeter)

가

s)

(blood - oxygen)

 (the rate of blood pulsation
 (non - invasive)

(photoelectrically)

(blood constituent)

5,259,381; 4,942,877; 4,446,715; 3,790,910; 4,303,984; 4,621,643; 5,246,003; 3,720,177; 4,684,245; 5,645,059; 5,058,588; 4,858,615; 4,942,877
(oximetry)

[illegible][illegible]

(c)

cosmic ray)
(electrostatic discharge)

(complex code)

(digital signature)

(entity)

가

(masking)

(Diffie - Hellman) (National Institute of Standards and Technology)
(Digital Signature Standard) , 가 (El Gamal)
, RSA (MIT (Massachusetts Institute of Technology)) - (Rabin - Williams)

가 (sign)

(digest)

가

ID,

(piece)

가

(mandatory bit)

가

가

(saturation calibration curve coefficient)

OFF (threshold)

(thermistor)

가

()

(symmetric
(Data Encr

ic key) (cryptographic algorithm),
ption Standard) (DES)

NIST

1
2
3
4
5
6
7
8
9
10

1

3

4

(flow)

7

가

(SIGNED DATA) (digest) ((hash function))
(digital signature)

가

가

(masking process)가

(MASKED DATA) , 가
(unmasking key)

가

(,)가
(message digest)

/ (SENSOR READER/MONITOR)

/ (SENSOR READER/MONITOR)

1 (non - invasive) (15) (pulse oximeter) 1 (18) LED(14)
 (18) 가 , (18) , (ph
 otosensor)(16) LED
 (16) , (input amplifier)(20)

LED (light source)가 , 가 , (white
 light source)가 (wavelength filter)

(Time Processing Unit) (48) LED 가 ,
 LED (32) , 가 ,
 LED
 (20) 1 , N N
 , (40), (low pass filter)(42) A/D (38)
 . TPU(48) (control line) LED(14)가 (in synchronizat
 ion) (queued serial module)(QSM)(46) A/D
 (data line) . CPU(50) QSM(46)
 QSM(46) RAM(52) , QSM(46), TPU(48), CPU(50)
 RAM(52)

(Sensor Memory)

(Sensor Memory)

(15) (16) LED(14) , (12) (12)
 (sensor reader) (17) CPU(50) . (12) (15) (12)
 , (12)
 , (12) (content)
 , (12) (12)
 , (12) 가 (extension cable)
 1 (disposable sensor) , (12) 가
 가 1

2 (12) (digital s
 ignature)(60) ,
 (62) (64) (,
) , (66)
 . (66) 가
 , (12)가 ,
 , , ,

(12)

3 (12)
 or)(72) 3 (72) (PC)(70) (cryptographic coprocess
 (private)/ (public)
 가 (72) PC(70) (72)

LED (72) (thermistor) (78),
 (76)가
 (80) PC 가 (82)
 (84)
 (serial number), (lot number),

(12) PC (72)
 (72) 가
 PC(70) PC(70)
 (86)
 (12)

4 3 5 4
 (sort)(90) LED 1 (91) (88)가 (92) 3
 (93) (decryption) 가 (91, 92, 93) 가
 (95) (91, 92, 93) (91, 92, 93) (94)
 (hash function)
 CRC 가 (91, 92, 93) 가
 2 가
 SHA - 1
 (Federal Information Processing Standard Publication) FIPS, PUB 180 - 1, S
 HA(Secure Hash Standard), (National Institute of Standards & Techonlogy), 1995

(95) (91) 96 (101) 100 가 (formatting data)(99) . 100 가 (92) 103 (101), (103) (93) (72) PC(70)

(12) .

(91) - (Rabin - Williams)

, 가 ISO 9796 - 2 .

, (91) 73 (byte) 20

(99) 3 96 .

, 128 106 가 (91) .

/ /

6 (17)

112) , CPU(50) (110) (

(114) .

7 6 . 8 7

(102) 8 (101), (107) 106 (93) .

(112)가 (108). .

(91) (95) (109) (cryptographic transform) .

(92) (107) (116) .

(91, 92, 93) , 2 (91),

(92) (93) (118) (120).

(122) 124 (95)(

) ((91, 92, 93))가

(126). . ,

(128).

, / 가 () ,

, (specification) 가

9 (91), (95) (99) , ID(13
 (91) CRC(134) (132) 1 ID(13
 6) , ID (bit)(138) 가
 (140) 7 가 ,
 (142) .
 , 가 ID(136)
 (140) ,
 가 (138)
 . ,
 . ,
 .
 (packing) ,
 가 .
 , (field identifier) " (escape character)"
 , 가 ,
 가, , , (stretch) .
 (12) .
 LED . 가
 (calibration curve) .
 , LED 가 , LED , 2
 , LED 가 .
 가
 .
 (12) , (traceability) , LED
 (bad sensor flag), , , LED
 V/I , LED , LED , (revision) (
), ID, / (adult/neonatal query flag)(
), 1 / (write once/write many flag), , (recycle event)
 .
 , (92),
 (91) (93) .

10 (202) (adapter) 10 (204)
 (206) (signal conditionin
 g circuitry) (208), 가 (210) (212)
 (206)
 , 가

10 (212) (dis
 play) (206)
 08) 가 (2
 (206)가 (212) (206) (214)
 (202)
 (212) (208) (206) AC
 가 (212)

가
 (57)

1.

;

가

가

(digital signature)

2.

1

(private key)

(sign)

(public key)

3.

1

I Gamal) - (Rabin - Williams) , RSA , - (Diffie - Hellman) , 가 (E

4.

1 ,

5.

4 ,

(masked) (symmetric key)

6.

5 ,

가 (hash function) (digest) ,

7.

6 ,

가 .

8.

7 ,

(unmasked) , ,

9.

1 ,

가 가 , (decode)
가 .

10.

9 ,

(message digest)

11.

1 ,
 가 / (bit) (flag) , (reading)
 가

12.

1 ,
 가 (pulse oximeter) , 가
 가 (saturation calculation coefficients), OFF (sensor OFF threshold)
 (thermistor calibration coefficients)

13.

12 ,

가 (lot code), (component) , L
 ED V/I , LED , (detector) , LED , (r
 evision) , 1 / , (recycle even
 ts) / (adult/neonatal query flag)

14.

:

;

;

15.

14 ,

(public key) (private key) ;

(sensor reader) ;

16.

14 ,

- (Rabin - Williams) , RSA , - (Diffie - Hellman) , 가 (E I Gamal)

17.

14 ,

(imbedding)

18.

14 ,

19.

14 ,

20.

19 ,

21.

20 ,

가

22.

21 ,

(unmasked)

23.

(sensor reader) ,

(housing);

;

;

,

;

1

;

(verification key)

2

;

3

;

(transfer circuit)

24.

23

,

1

2

가

25.

23

,

가

26.

23

,

가

27.

23

,

- (Rabin - Williams)

28.

23

,

가

29.

,

(a)

,

,

,

,

가 ,

,

(b)

,

;

;

;

;

1

;

2

;

3

,

.

30.

,

;

/

;

;

가

가

가

;

가

가

가

,

.

31.

30

,

(field length)

;

;

가

가

가

.

32.

1

,

가

(adapter)

.

33.

14

,

가

(adapter)

.

34.

29

,

가

(adapter)

.

35.

;

,

,

.

36.

35

,

;

2 ,

가

(conditioning circuit)

.

37.

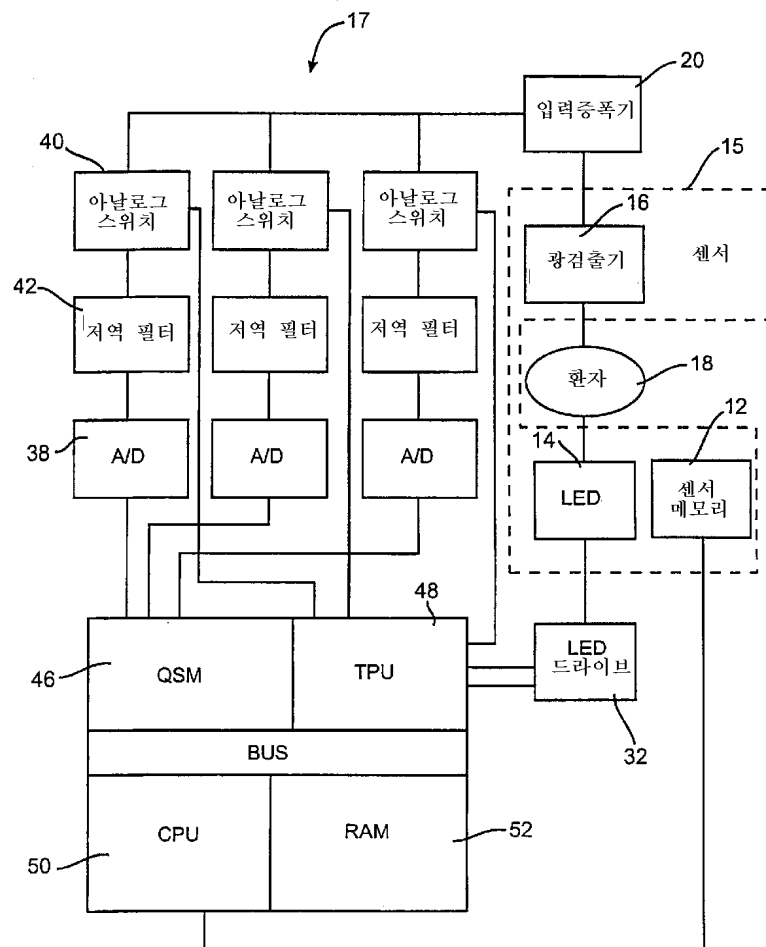
1 ;

2

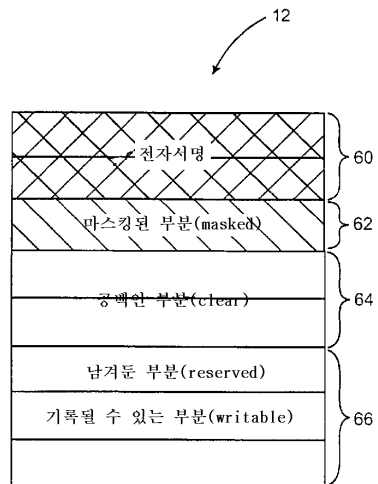
38.

;

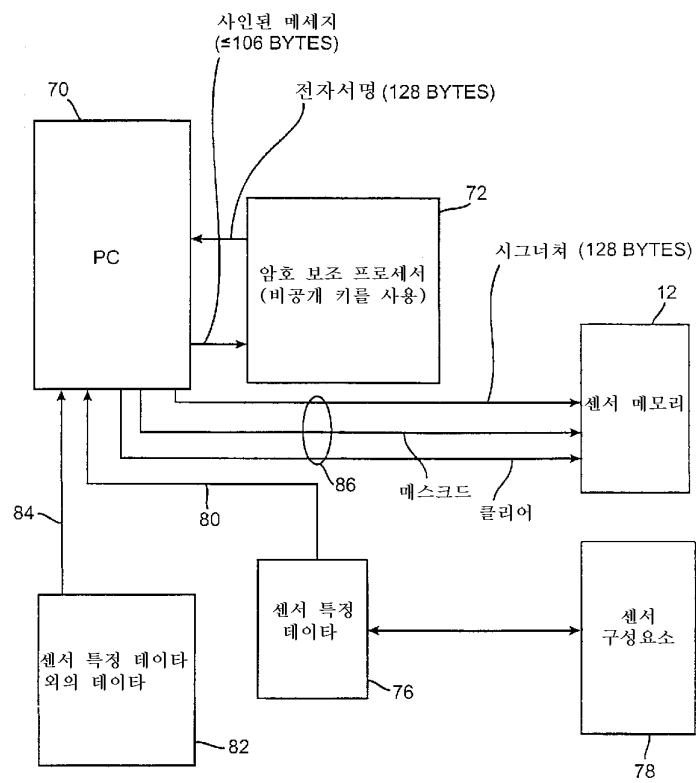
1



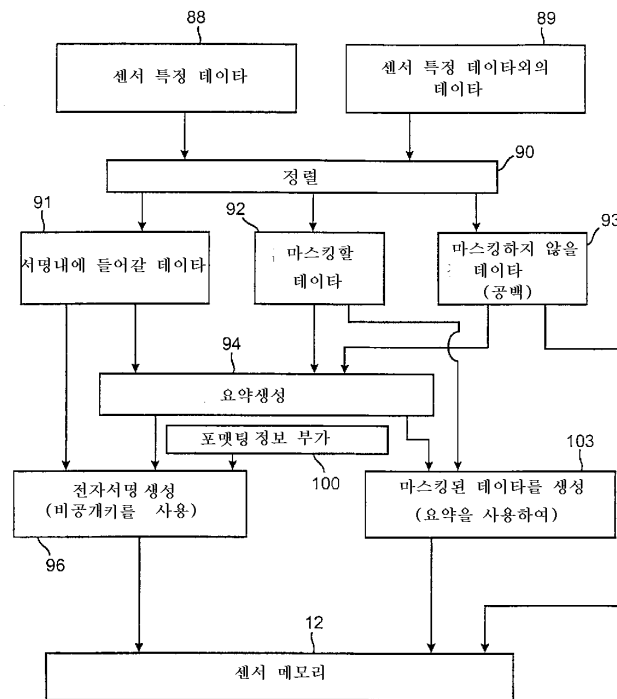
2



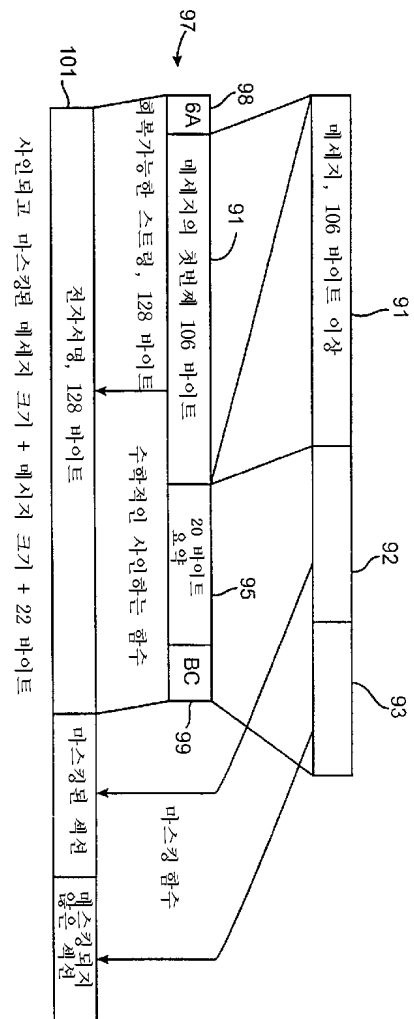
3



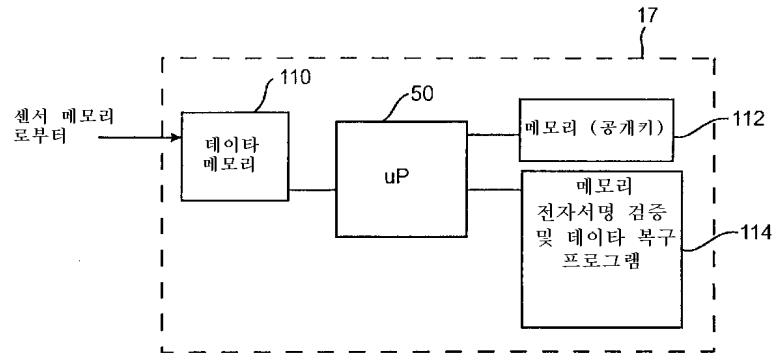
4



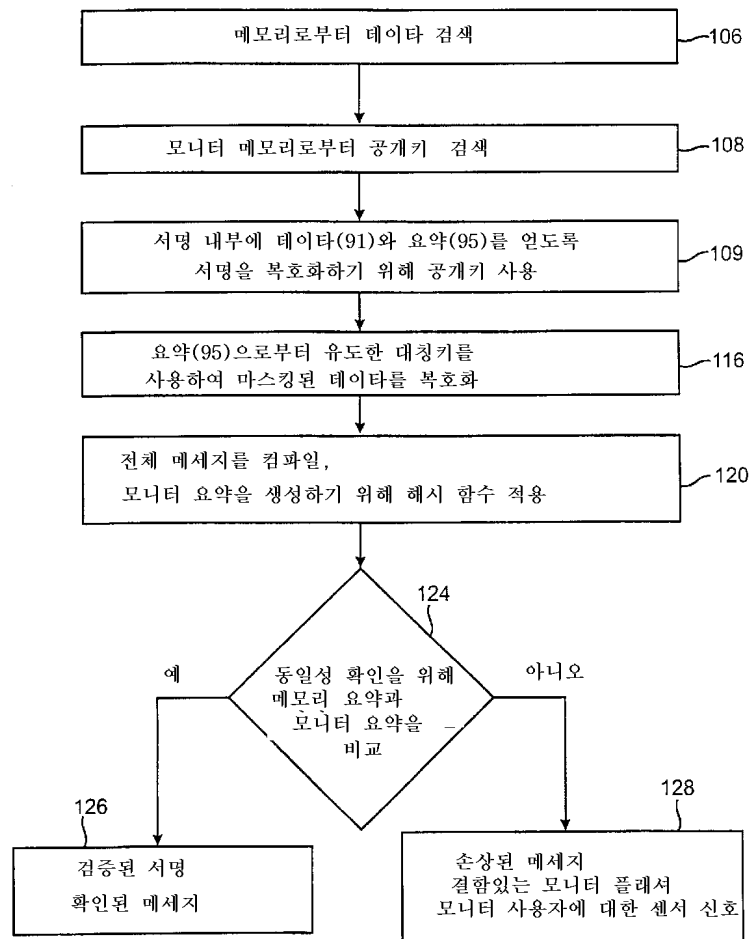
5



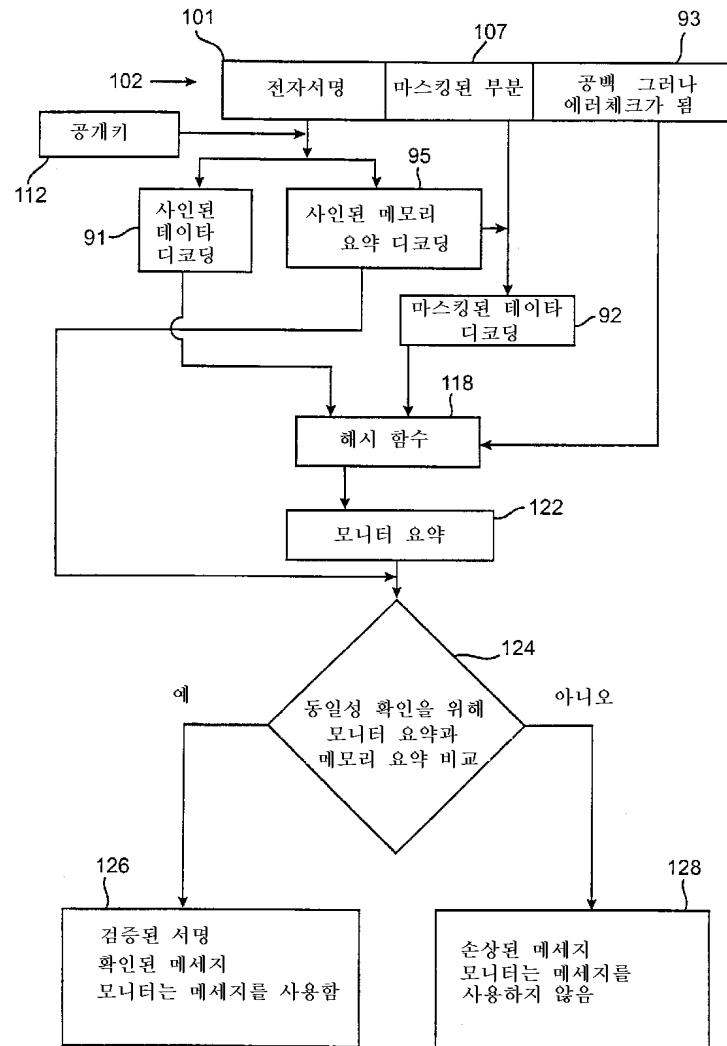
6

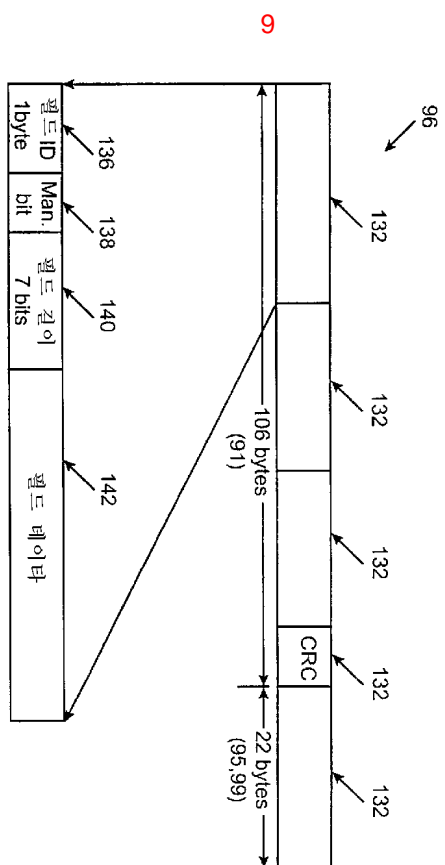


7

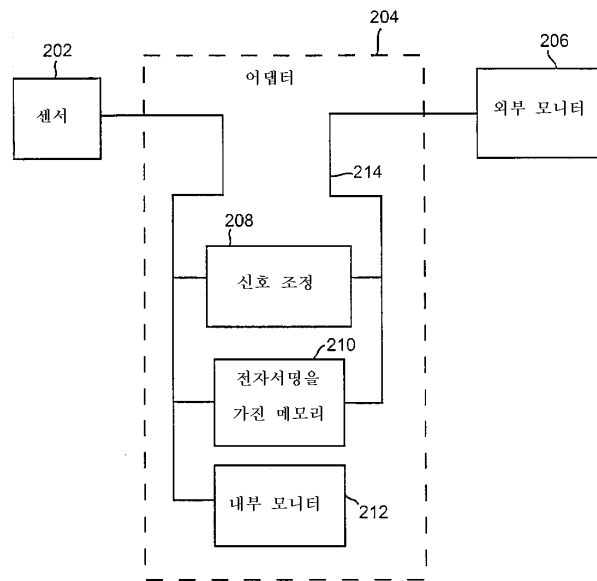


8





10



| | | | |
|----------------|--|---------|------------|
| 专利名称(译) | 具有与传感器相关的数据的数字签名的传感器 | | |
| 公开(公告)号 | KR1020020064292A | 公开(公告)日 | 2002-08-07 |
| 申请号 | KR1020027004038 | 申请日 | 2000-09-28 |
| [标]申请(专利权)人(译) | 马林克罗特公司 | | |
| 申请(专利权)人(译) | 每天的大批量埃尔埃尔先生 | | |
| 当前申请(专利权)人(译) | 每天的大批量埃尔埃尔先生 | | |
| [标]发明人 | BERSON THOMAS A 버슨토마스에이 OLSON BRYAN 올슨브라이언 FEIN MICHAEL E 페인마이클이 MANNHEIMER PAUL D 맨하이머폴디 PORGES CHARLES E 포제스찰스이 SCHLOEMER DAVID 쉬로머데이비드 | | |
| 发明人 | 버슨,토마스,에이. 올슨,브라이언 페인,마이클,이. 맨하이머,폴,디. 포제스,찰스,이. 쉬로머,데이비드 | | |
| IPC分类号 | A61B5/145 A61B5/00 A61B5/1455 G06F1/00 G06F12/14 G06F21/24 H04L9/32 | | |
| CPC分类号 | A61B5/14551 A61B2562/08 G06F21/64 G06F2211/008 G06F2221/2107 H04L9/3247 H04L2209/805 A61B2562/085 G06F21/6209 H04L2209/88 | | |
| 优先权 | 09/662246 2000-09-14 US 60/156488 1999-09-28 US | | |
| 其他公开文献 | KR100679762B1 | | |
| 外部链接 | Espacenet | | |

摘要(译)

g data) (99) 。在步骤100添加格式化数据，例如根据国际标准ISO / IEC 9796-2，数字签名的标准。在步骤103中屏蔽数据92。然后，该签名101，屏蔽数据103和空白数据93由PC 70与协处理器72组合，

