163163

G00002

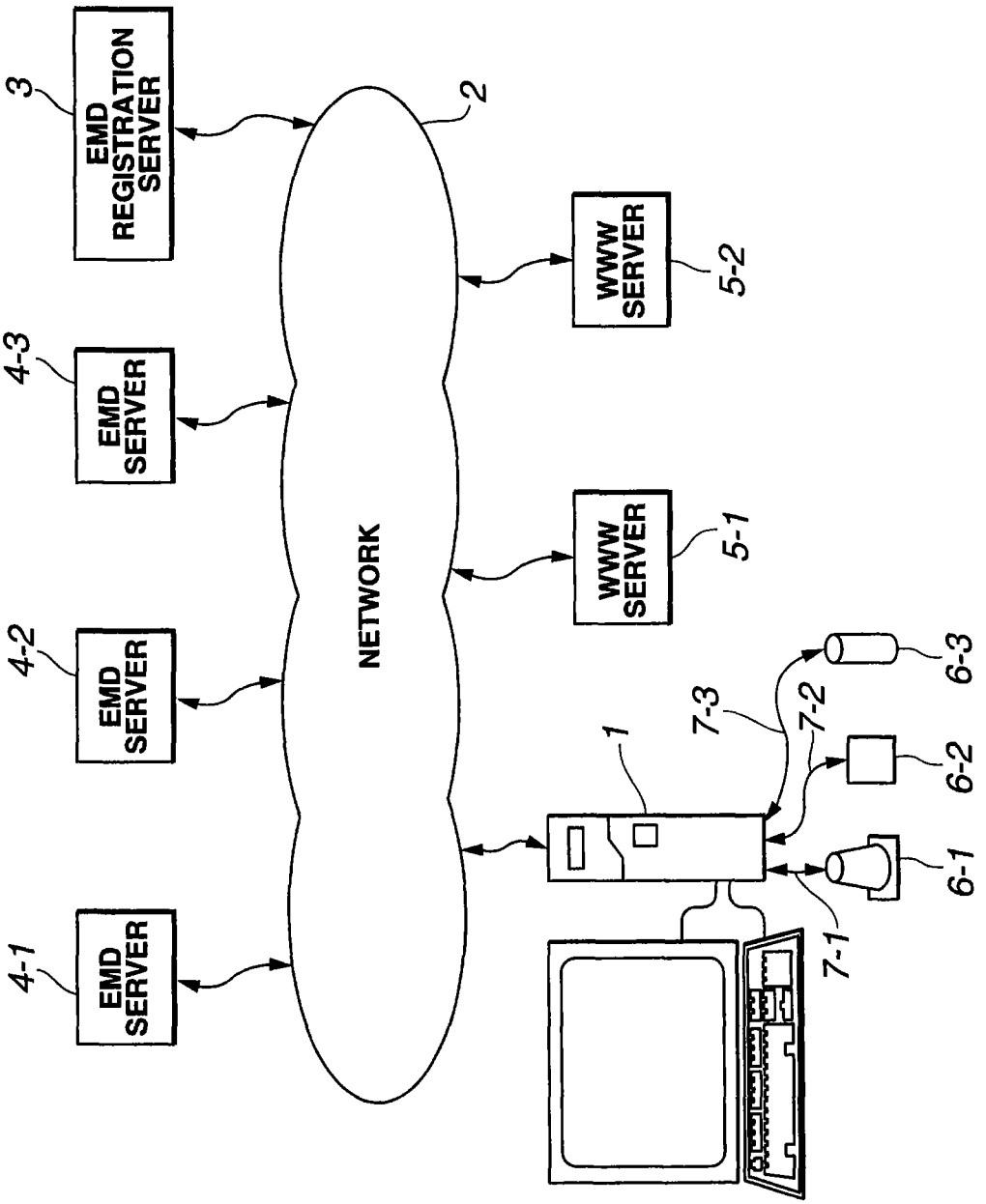


FIG.1

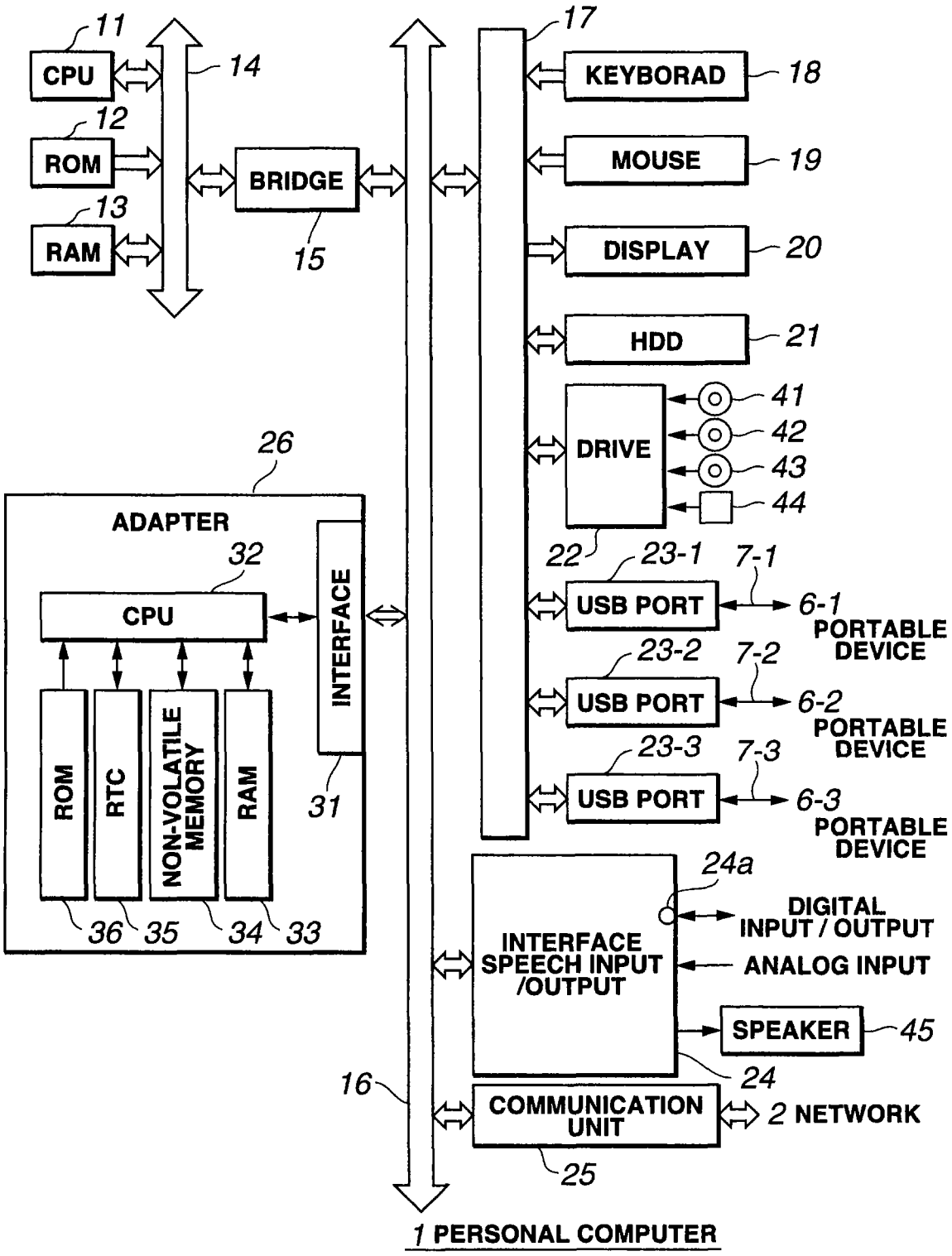

11
CPU
12
ROM
13
RAM
14
BRIDGE
15
16
17
KEYBORAD
18
MOUSE
19
DISPLAY
20
HDD
21
DRIVE
41
42
43
44
22
23-1
USB PORT
7-1
6-1
PORTABLE DEVICE
23-2
USB PORT
7-2
6-2
PORTABLE DEVICE
23-3
USB PORT
7-3
6-3
PORTABLE DEVICE
24a
DIGITAL INPUT / OUTPUT
INTERFACE SPEECH INPUT /OUTPUT
ANALOG INPUT
SPEAKER
45
24
COMMUNICATION UNIT
2 NETWORK
25
26
ADAPTER
32
CPU
INTERFACE
31
ROM
RTC
NON-VOLATILE MEMORY
RAM
36
35
34
33
1 PERSONAL COMPUTER

FIG.2

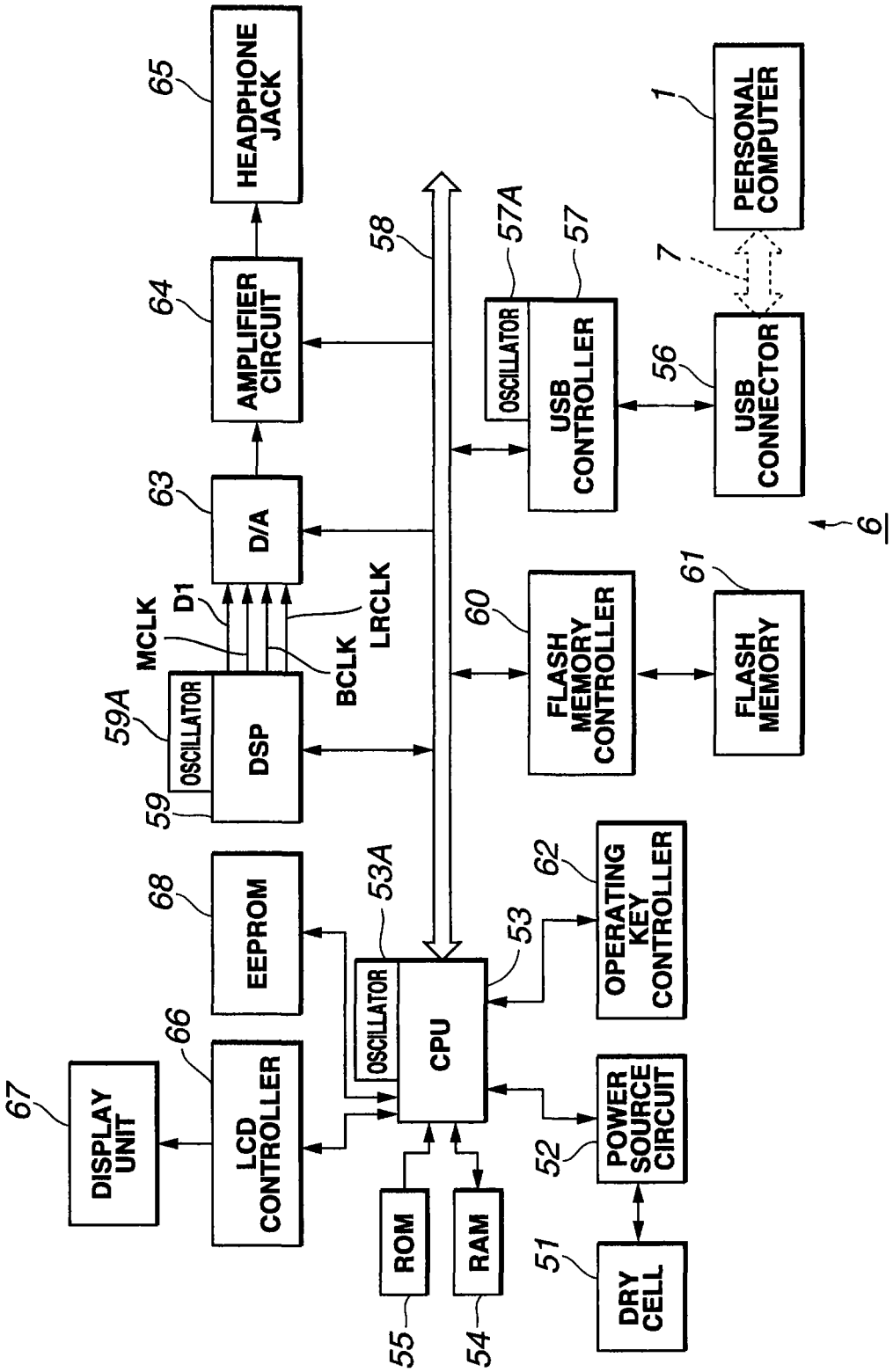

HEADPHONE JACK
65
AMPLIFIER CIRCUIT
64
D/A
63
MCLK
D1
BCLK
LRCLK
OSCILLATOR
DSP
59A
59
58
57A
57
OSCILLATOR
USB CONTROLLER
56
USB CONNECTOR
7
PERSONAL COMPUTER
1
6
60
FLASH MEMORY CONTROLLER
61
FLASH MEMORY
EEPROM
68
53A
OSCILLATOR
CPU
53
62
OPERATING KEY CONTROLLER
66
LCD CONTROLLER
67
DISPLAY UNIT
ROM
55
RAM
54
52
POWER SOURCE CIRCUIT
51
DRY CELL

FIG.3

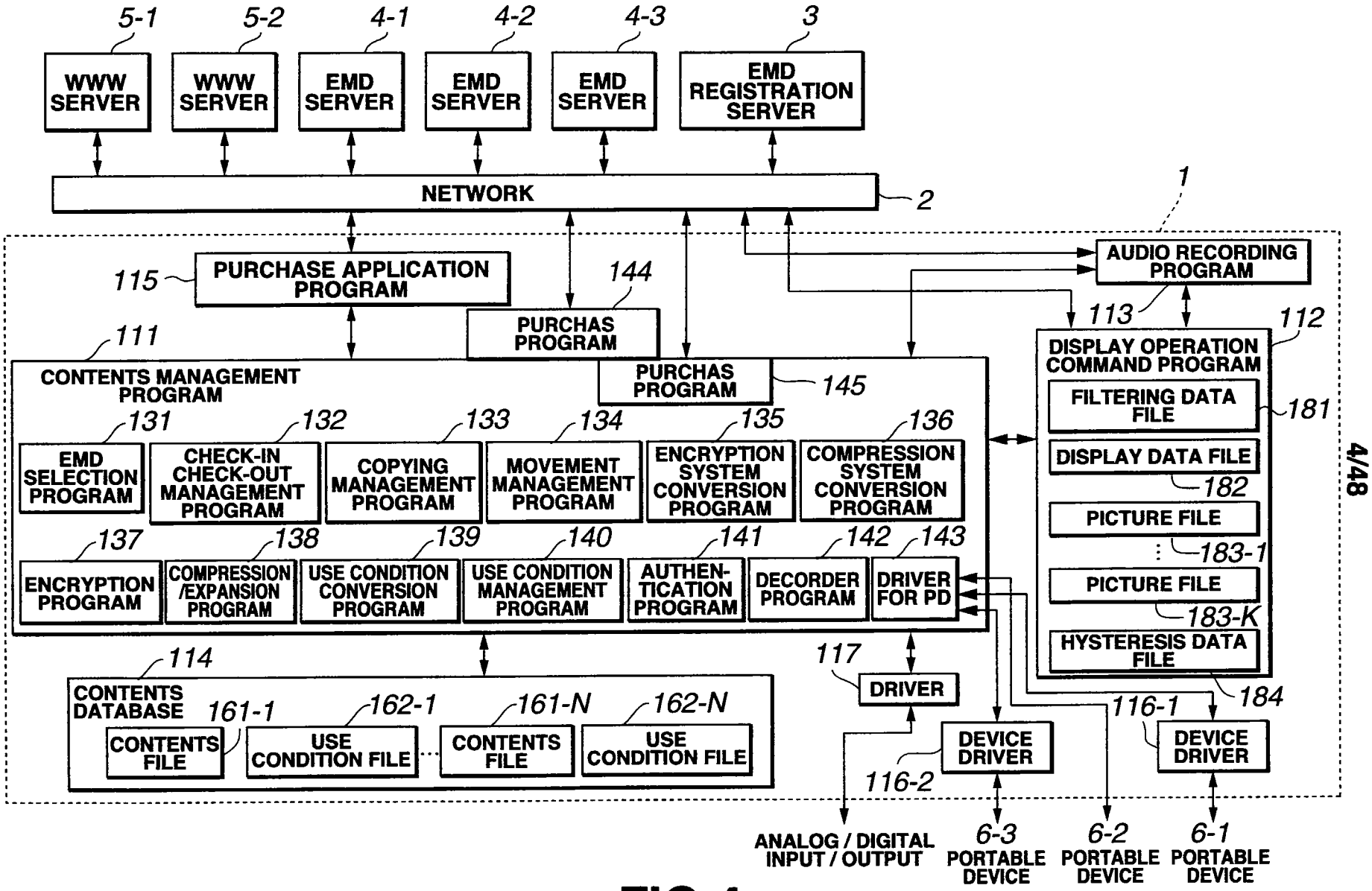

5-1
5-2
4-1
4-2
4-3
3
WWW SERVER
WWW SERVER
EMD SERVER
EMD SERVER
EMD SERVER
EMD REGISTRATION SERVER
NETWORK
2
1
AUDIO RECORDING PROGRAM
115
PURCHASE APPLICATION PROGRAM
144
PURCHAS PROGRAM
113
112
111
DISPLAY OPERATION COMMAND PROGRAM
CONTENTS MANAGEMENT PROGRAM
PURCHAS PROGRAM
145
FILTERING DATA FILE
181
131
132
133
134
135
136
EMD SELECTION PROGRAM
CHECK-IN CHECK-OUT MANAGEMENT PROGRAM
COPYING MANAGEMENT PROGRAM
MOVEMENT MANAGEMENT PROGRAM
ENCRYPTION SYSTEM CONVERSION PROGRAM
COMPRESSION SYSTEM CONVERSION PROGRAM
DISPLAY DATA FILE
182
PICTURE FILE
183-1
137
138
139
140
141
142
143
ENCRYPTION PROGRAM
COMPRESSION /EXPANSION PROGRAM
USE CONDITION CONVERSION PROGRAM
USE CONDITION MANAGEMENT PROGRAM
AUTHEN-TICATION PROGRAM
DECORDER PROGRAM
DRIVER FOR PD
PICTURE FILE
183-K
HYSTERESIS DATA FILE
184
4/48
114
117
CONTENTS DATABASE
DRIVER
161-1
162-1
161-N
162-N
116-1
CONTENTS FILE
USE CONDITION FILE
CONTENTS FILE
USE CONDITION FILE
DEVICE DRIVER
DEVICE DRIVER
116-2
ANALOG / DIGITAL INPUT / OUTPUT
6-3 PORTABLE DEVICE
6-2 PORTABLE DEVICE
6-1 PORTABLE DEVICE

FIG.4

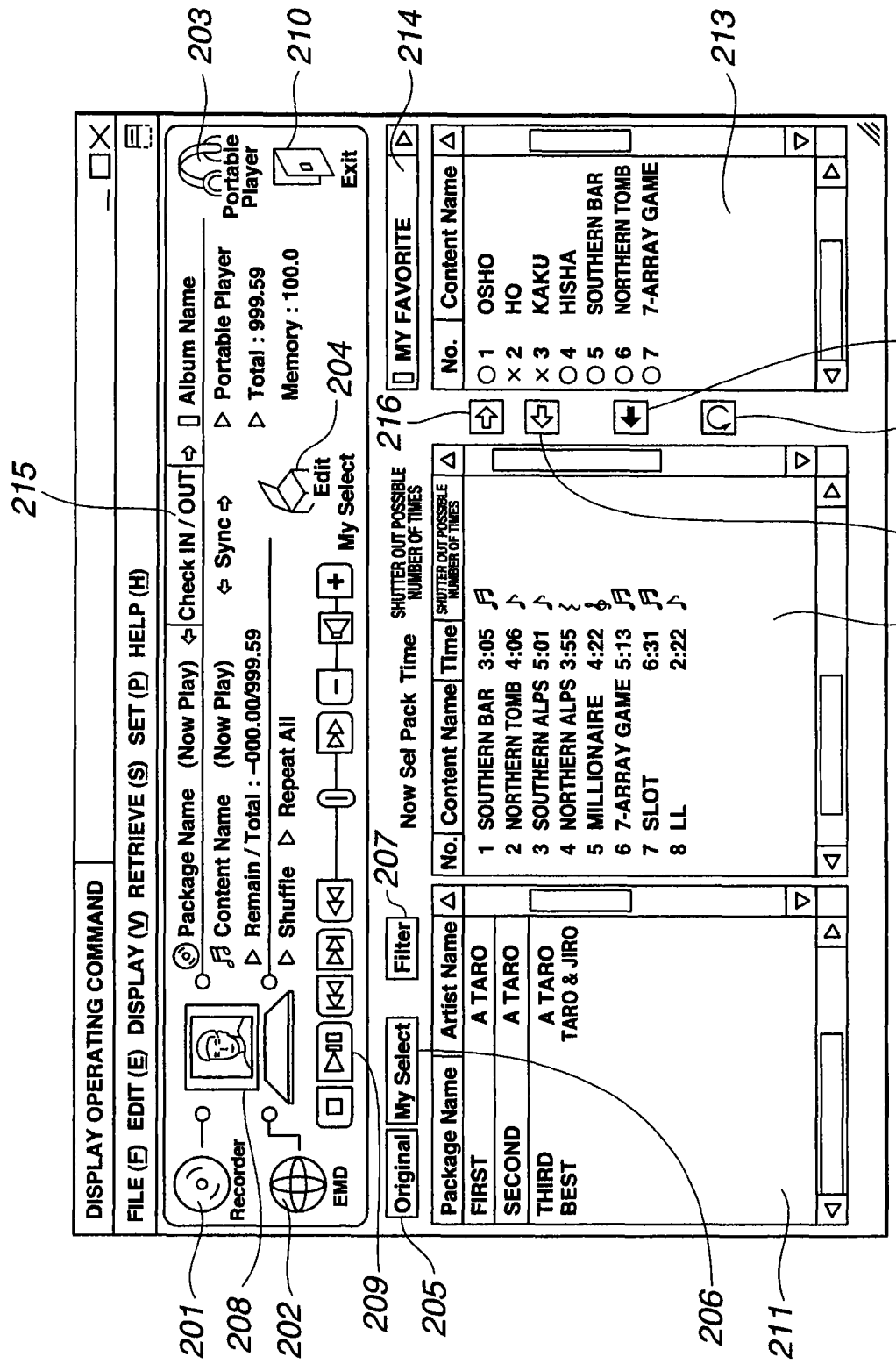

DISPLAY OPERATING COMMAND
FILE (F) EDIT (E) DISPLAY (V) RETRIEVE (S) SET (P) HELP (H)
Package Name (Now Play)
Content Name (Now Play)
Remain / Total : -000.00/999.59
Shuffle
Repeat All
Check IN / OUT
Sync
Album Name
Portable Player
Total : 999.59
Memory : 100.0
Edit
My Select
Portable Player
Exit
Recorder
EMD
Original
My Select
Filter
MY FAVORITE
Now Sel Pack Time
SHUTTER OUT POSSIBLE NUMBER OF TIMES
Package Name
Artist Name
FIRST A TARO
SECOND A TARO
THIRD A TARO
BEST TARO & JIRO
No. Content Name Time
1 SOUTHERN BAR 3:05
2 NORTHERN TOMB 4:06
3 SOUTHERN ALPS 5:01
4 NORTHERN ALPS 3:55
5 MILLIONAIRE 4:22
6 7-ARRAY GAME 5:13
7 SLOT 6:31
8 LL 2:22
No. Content Name
1 OSHO
2 HO
3 KAKU
4 HISHA
5 SOUTHERN BAR
6 NORTHERN TOMB
7 7-ARRAY GAME
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219

FIG.5

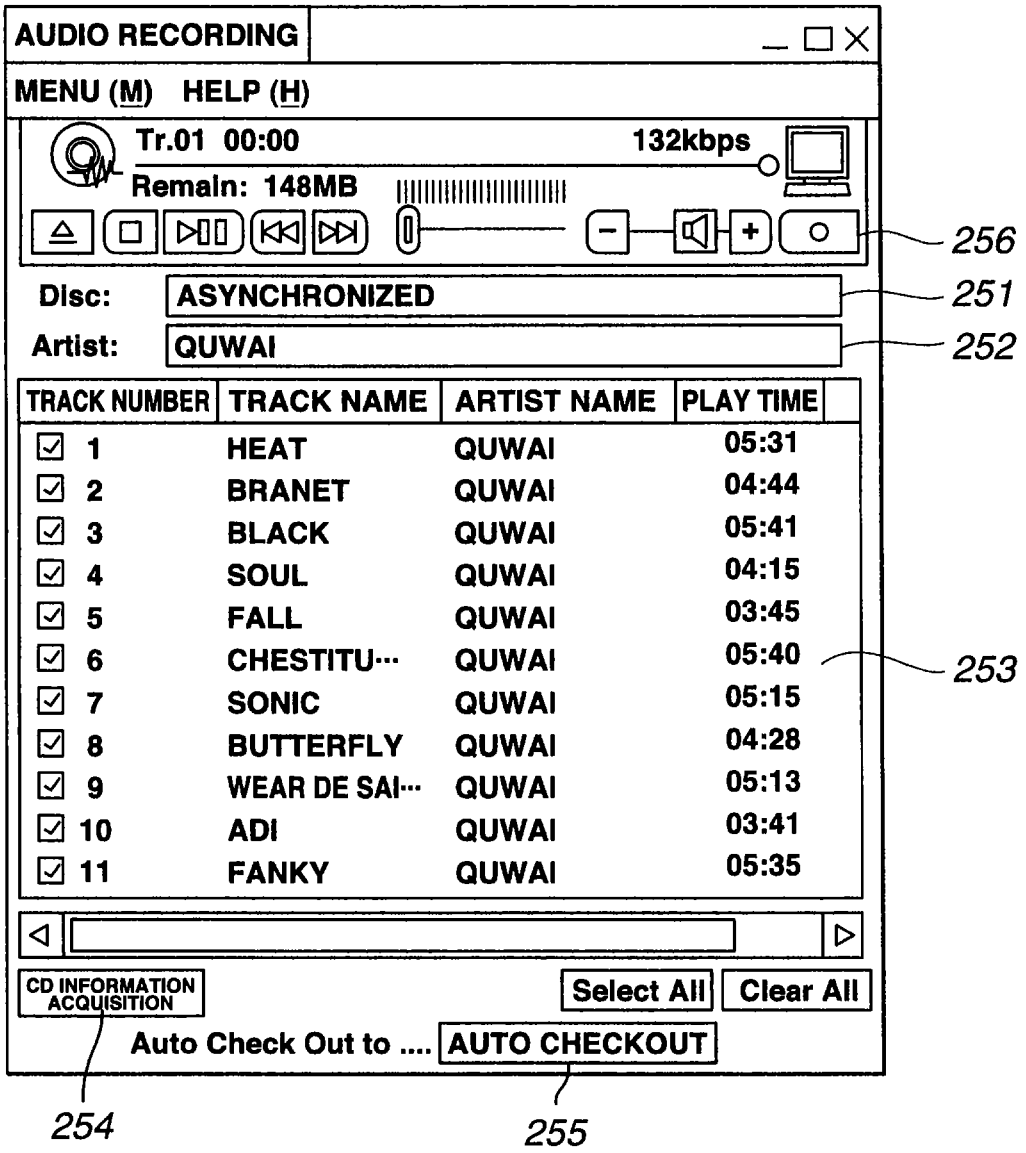

AUDIO RECORDING
MENU (M) HELP (H)
Tr.01 00:00
132kbps
Remain: 148MB
Disc: ASYNCHRONIZED
Artist: QUWAI
TRACK NUMBER
TRACK NAME
ARTIST NAME
PLAY TIME
1 HEAT QUWAI 05:31
2 BRANET QUWAI 04:44
3 BLACK QUWAI 05:41
4 SOUL QUWAI 04:15
5 FALL QUWAI 03:45
6 CHESTITU··· QUWAI 05:40
7 SONIC QUWAI 05:15
8 BUTTERFLY QUWAI 04:28
9 WEAR DE SAI··· QUWAI 05:13
10 ADI QUWAI 03:41
11 FANKY QUWAI 05:35
CD INFORMATION ACQUISITION
Select All
Clear All
Auto Check Out to .... AUTO CHECKOUT
256
251
252
253
254
255

FIG.6

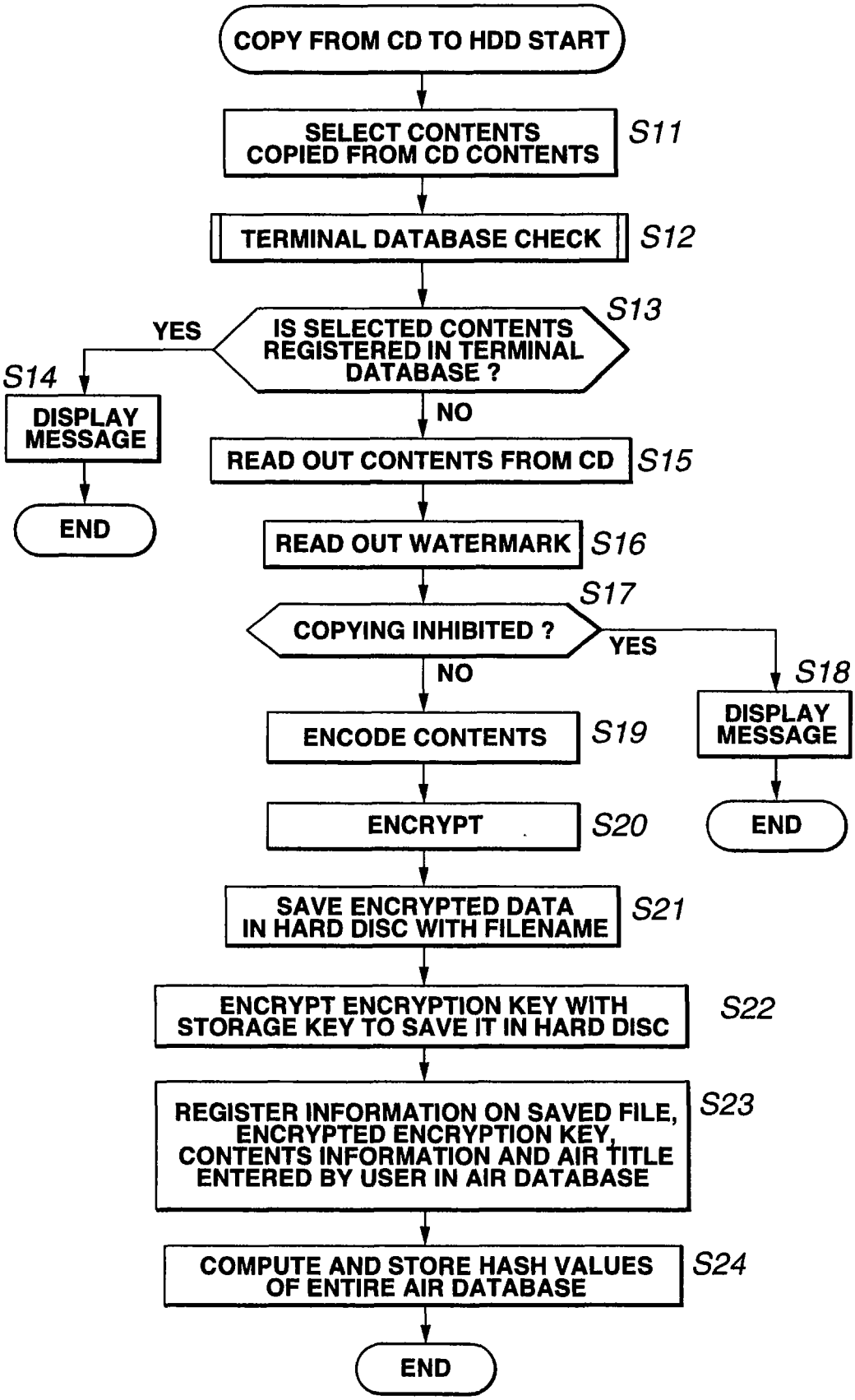

COPY FROM CD TO HDD START
SELECT CONTENTS COPIED FROM CD CONTENTS
S11
TERMINAL DATABASE CHECK
S12
IS SELECTED CONTENTS REGISTERED IN TERMINAL DATABASE ?
S13
YES
S14
DISPLAY MESSAGE
END
NO
READ OUT CONTENTS FROM CD
S15
READ OUT WATERMARK
S16
COPYING INHIBITED ?
S17
YES
S18
DISPLAY MESSAGE
END
NO
ENCODE CONTENTS
S19
ENCRYPT
S20
SAVE ENCRYPTED DATA IN HARD DISC WITH FILENAME
S21
ENCRYPT ENCRYPTION KEY WITH STORAGE KEY TO SAVE IT IN HARD DISC
S22
REGISTER INFORMATION ON SAVED FILE, ENCRYPTED ENCRYPTION KEY, CONTENTS INFORMATION AND AIR TITLE ENTERED BY USER IN AIR DATABASE
S23
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S24
END

FIG.7

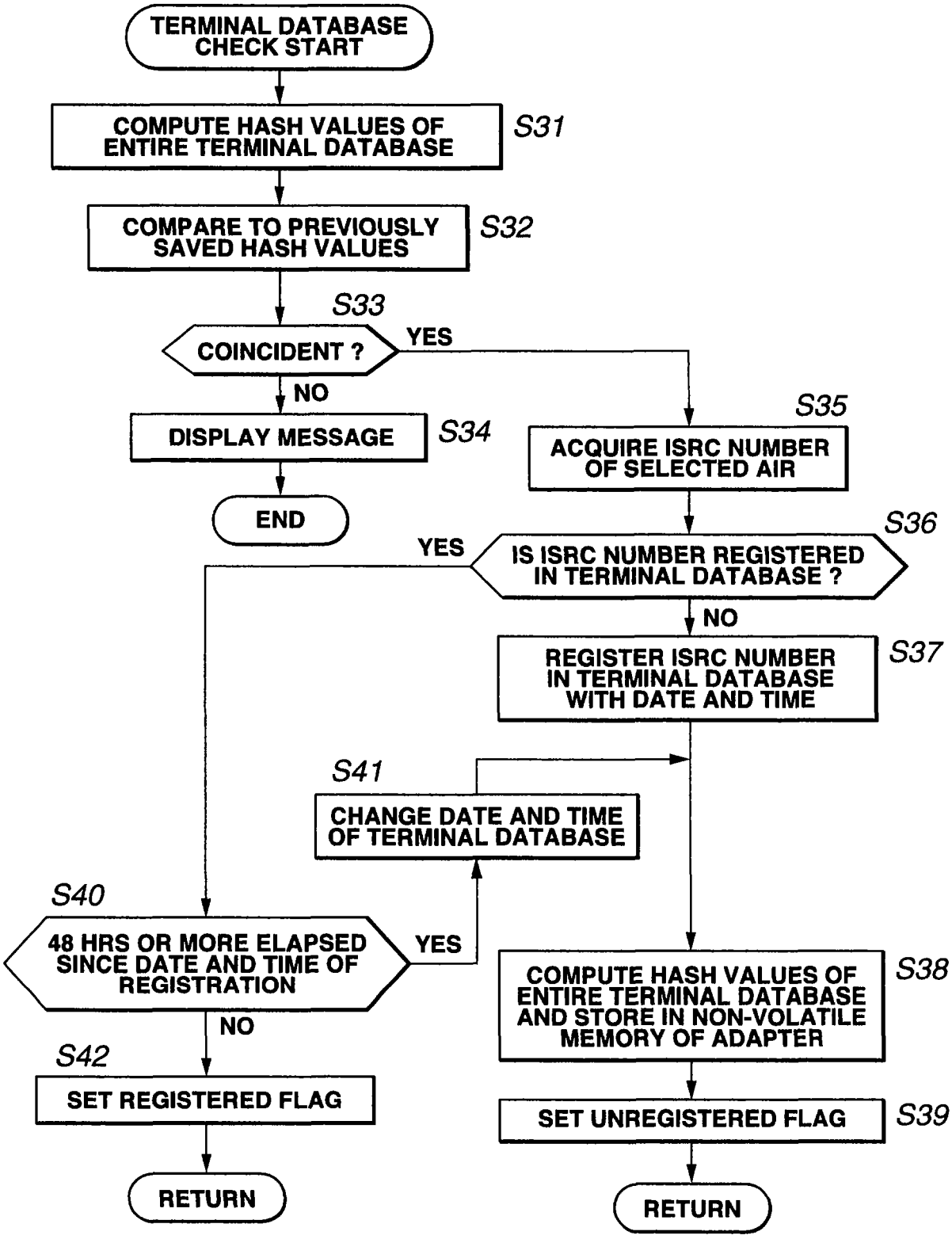

TERMINAL DATABASE CHECK START
COMPUTE HASH VALUES OF ENTIRE TERMINAL DATABASE
S31
COMPARE TO PREVIOUSLY SAVED HASH VALUES
S32
S33
COINCIDENT ?
YES
NO
DISPLAY MESSAGE
S34
END
S35
ACQUIRE ISRC NUMBER OF SELECTED AIR
S36
IS ISRC NUMBER REGISTERED IN TERMINAL DATABASE ?
YES
NO
REGISTER ISRC NUMBER IN TERMINAL DATABASE WITH DATE AND TIME
S37
S41
CHANGE DATE AND TIME OF TERMINAL DATABASE
S40
48 HRS OR MORE ELAPSED SINCE DATE AND TIME OF REGISTRATION
YES
NO
S42
SET REGISTERED FLAG
RETURN
COMPUTE HASH VALUES OF ENTIRE TERMINAL DATABASE AND STORE IN NON-VOLATILE MEMORY OF ADAPTER
S38
SET UNREGISTERED FLAG
S39
RETURN

FIG.8

TERMINAL DATABASE

	ITEM 1	ITEM 2	ITEM 3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
COPYING DATE AND TIME	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16:15	

HASH VALUES	Oxf3352e125934

FIG.9

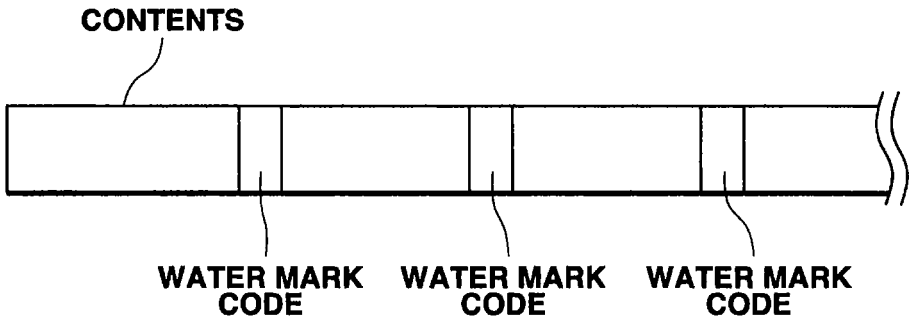


FIG.10

AIR DATABASE

	ITEM 1	ITEM 2	ITEM 3	
FILENAME	Xd000110. at2	px92341234. at2	aa0234287034. at2	
ENCRYPTED ENCRYPTION KEY	Oxabababababab	Ox9898989898989	Ox123456789012	
AIR TITLE	BROOK IN SPRINGTIME	SCHICKSAL	MOON OF FORLORN CASTLE	
DURATION	180	190	200	
PLAYBACK CONDITION : START DATE AND TIME	-	2001.01.01.00:00	-	
PLAYBACK CONDITION : END DATE AND TIME	1999.07.31.23:59	-	-	
PLAYBACK CONDITION : LIMITATION ON NUMBER OF TIMES	-	20	-	
NUMBER OF TIMES OF PLAYBACK COUNTER	-	12	-	
ON PLAYBACK CHARGING CONDITION	-	-	¥5	
COPYING CONDITIONS NUMBER OF TIMES	2	0	0	
COPYING NUMBER OF TIMES COUNTER	1	0	0	
COPYING CONDITIONS : SCMS	Ob01	Ob10	Ob00	

HASH VALUES	Oxf9951e566321

FIG.11

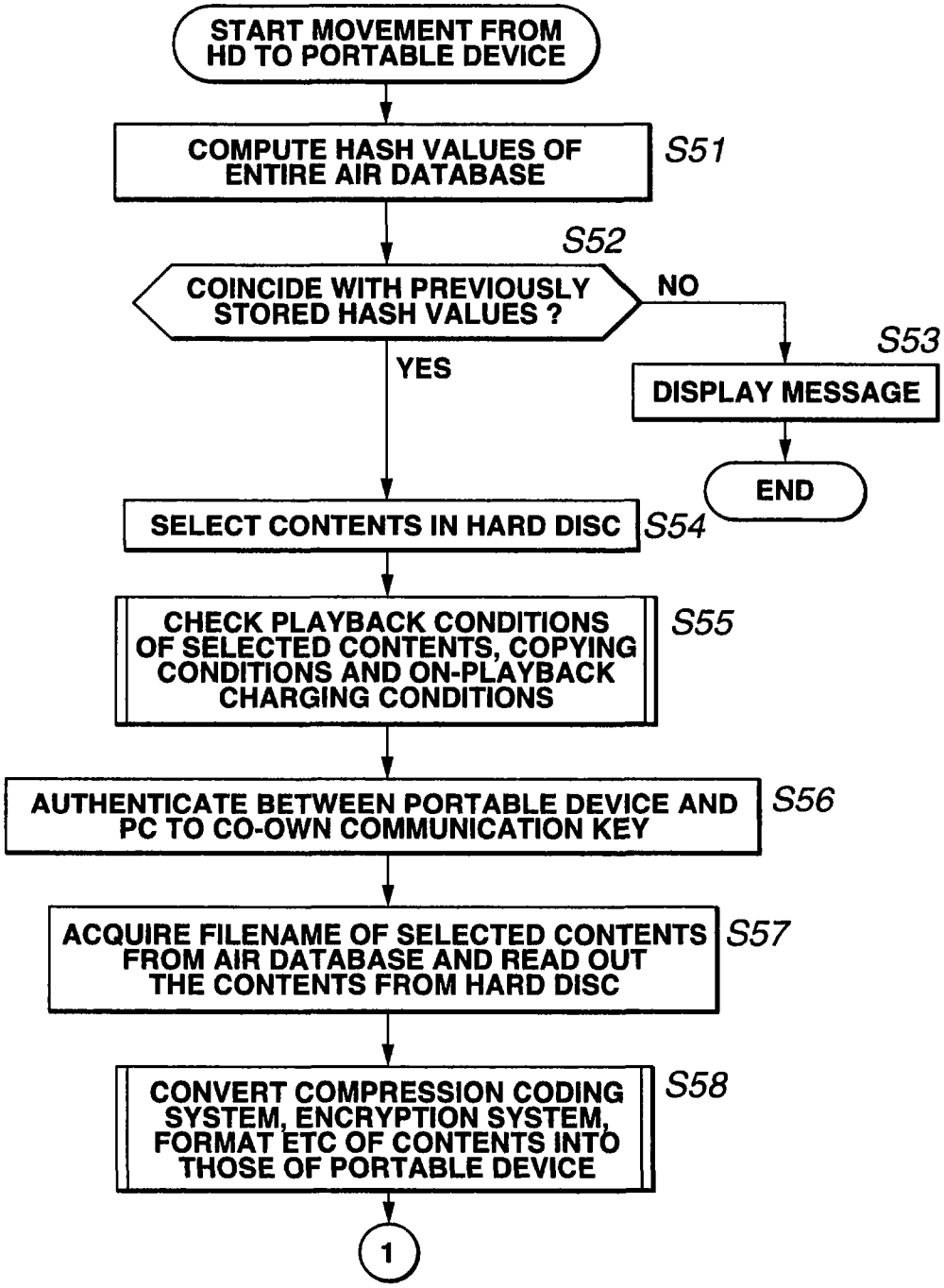

START MOVEMENT FROM HD TO PORTABLE DEVICE
COMPUTE HASH VALUES OF ENTIRE AIR DATABASE
S51
S52
COINCIDE WITH PREVIOUSLY STORED HASH VALUES ?
NO
S53
DISPLAY MESSAGE
END
YES
SELECT CONTENTS IN HARD DISC
S54
CHECK PLAYBACK CONDITIONS OF SELECTED CONTENTS, COPYING CONDITIONS AND ON-PLAYBACK CHARGING CONDITIONS
S55
AUTHENTICATE BETWEEN PORTABLE DEVICE AND PC TO CO-OWN COMMUNICATION KEY
S56
ACQUIRE FILENAME OF SELECTED CONTENTS FROM AIR DATABASE AND READ OUT THE CONTENTS FROM HARD DISC
S57
CONVERT COMPRESSION CODING SYSTEM, ENCRYPTION SYSTEM, FORMAT ETC OF CONTENTS INTO THOSE OF PORTABLE DEVICE
S58
1

FIG.12

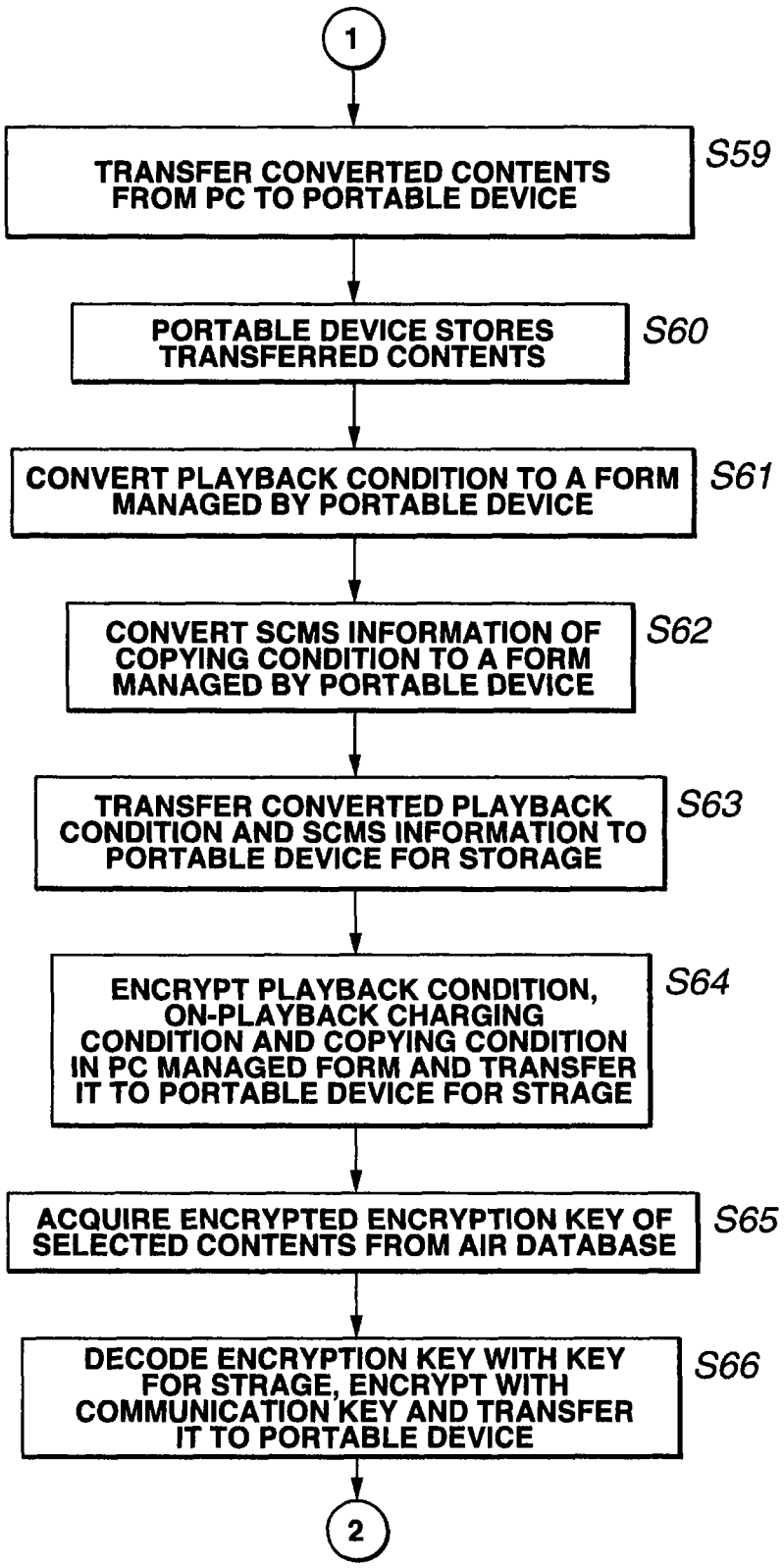

1
TRANSFER CONVERTED CONTENTS FROM PC TO PORTABLE DEVICE
S59
PORTABLE DEVICE STORES TRANSFERRED CONTENTS
S60
CONVERT PLAYBACK CONDITION TO A FORM MANAGED BY PORTABLE DEVICE
S61
CONVERT SCMS INFORMATION OF COPYING CONDITION TO A FORM MANAGED BY PORTABLE DEVICE
S62
TRANSFER CONVERTED PLAYBACK CONDITION AND SCMS INFORMATION TO PORTABLE DEVICE FOR STORAGE
S63
ENCRYPT PLAYBACK CONDITION, ON-PLAYBACK CHARGING CONDITION AND COPYING CONDITION IN PC MANAGED FORM AND TRANSFER IT TO PORTABLE DEVICE FOR STRAGE
S64
ACQUIRE ENCRYPTED ENCRYPTION KEY OF SELECTED CONTENTS FROM AIR DATABASE
S65
DECODE ENCRYPTION KEY WITH KEY FOR STRAGE, ENCRYPT WITH COMMUNICATION KEY AND TRANSFER IT TO PORTABLE DEVICE
S66
2

FIG.13

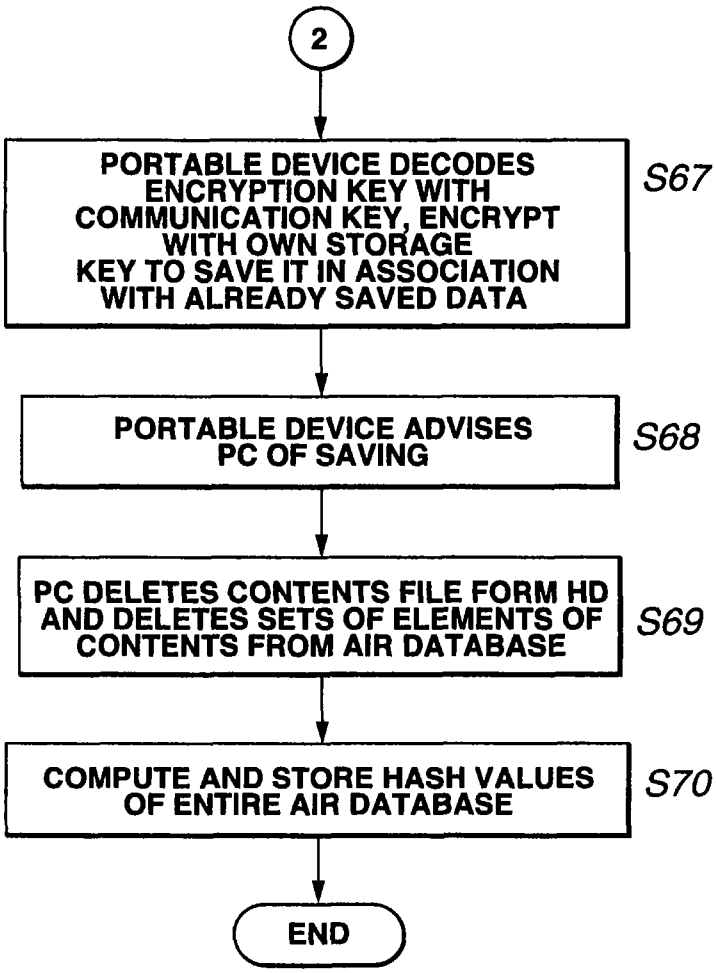

2
PORTABLE DEVICE DECODES ENCRYPTION KEY WITH COMMUNICATION KEY, ENCRYPT WITH OWN STORAGE KEY TO SAVE IT IN ASSOCIATION WITH ALREADY SAVED DATA
S67
PORTABLE DEVICE ADVISES PC OF SAVING
S68
PC DELETES CONTENTS FILE FORM HD AND DELETES SETS OF ELEMENTS OF CONTENTS FROM AIR DATABASE
S69
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S70
END

FIG.14

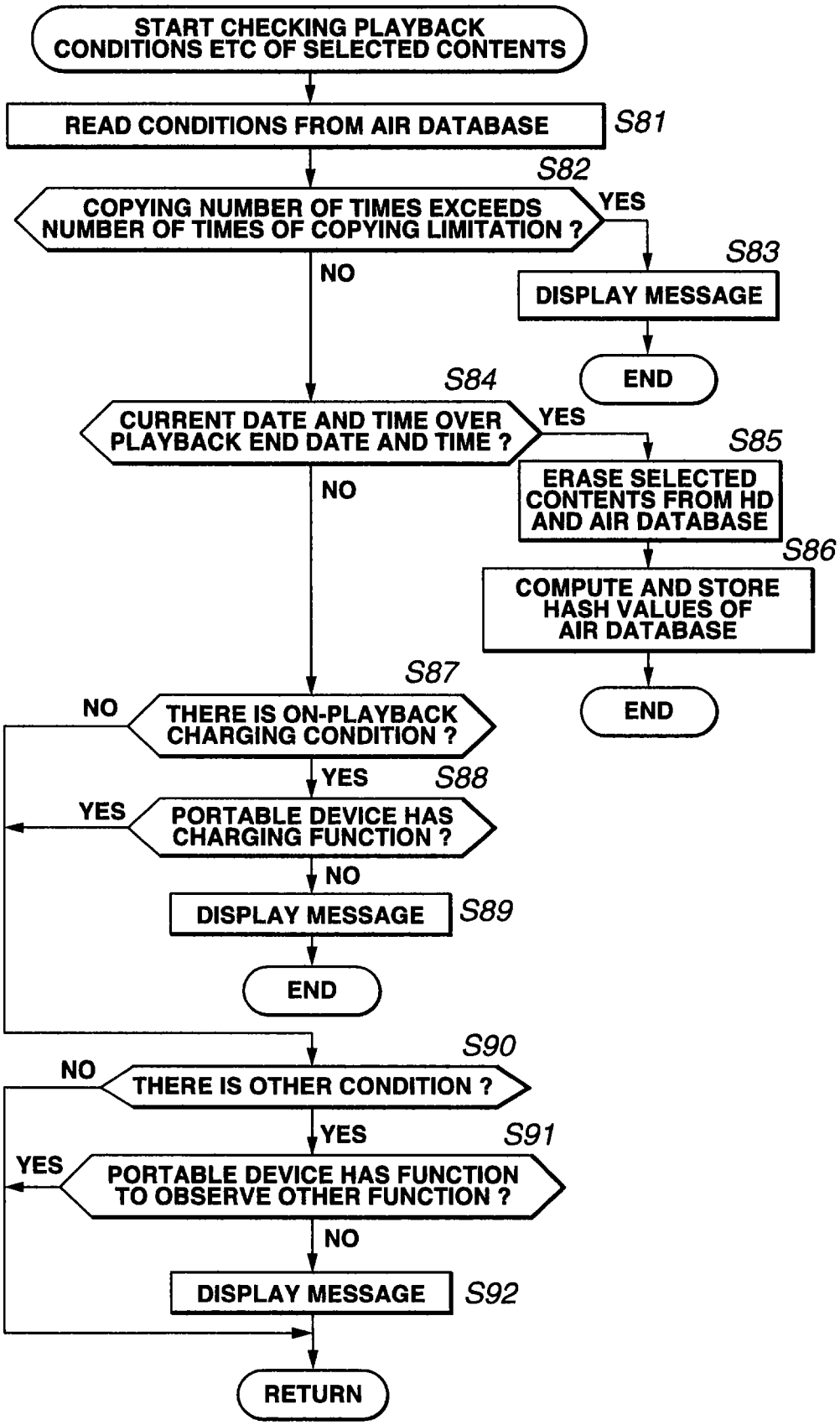

START CHECKING PLAYBACK CONDITIONS ETC OF SELECTED CONTENTS
READ CONDITIONS FROM AIR DATABASE
S81
S82
COPYING NUMBER OF TIMES EXCEEDS NUMBER OF TIMES OF COPYING LIMITATION ?
YES
NO
S83
DISPLAY MESSAGE
END
S84
CURRENT DATE AND TIME OVER PLAYBACK END DATE AND TIME ?
YES
NO
S85
ERASE SELECTED CONTENTS FROM HD AND AIR DATABASE
S86
COMPUTE AND STORE HASH VALUES OF AIR DATABASE
END
S87
NO
THERE IS ON-PLAYBACK CHARGING CONDITION ?
YES
S88
YES
PORTABLE DEVICE HAS CHARGING FUNCTION ?
NO
DISPLAY MESSAGE
S89
END
S90
NO
THERE IS OTHER CONDITION ?
YES
S91
YES
PORTABLE DEVICE HAS FUNCTION TO OBSERVE OTHER FUNCTION ?
NO
DISPLAY MESSAGE
S92
RETURN

FIG.15

PLAYBACK CONDITIONS MANAGED BY PORTABLE DEVICE

	ITEM 1	ITEM 2	ITEM 3
CONTENTS ID	00001	00002	00003
PLAYBACK START DATE & TIME	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
PLAYBACK END DATE & TIME	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
NUMBER OF TIMES OF PLAYBACK	-	15	-

FIG.16

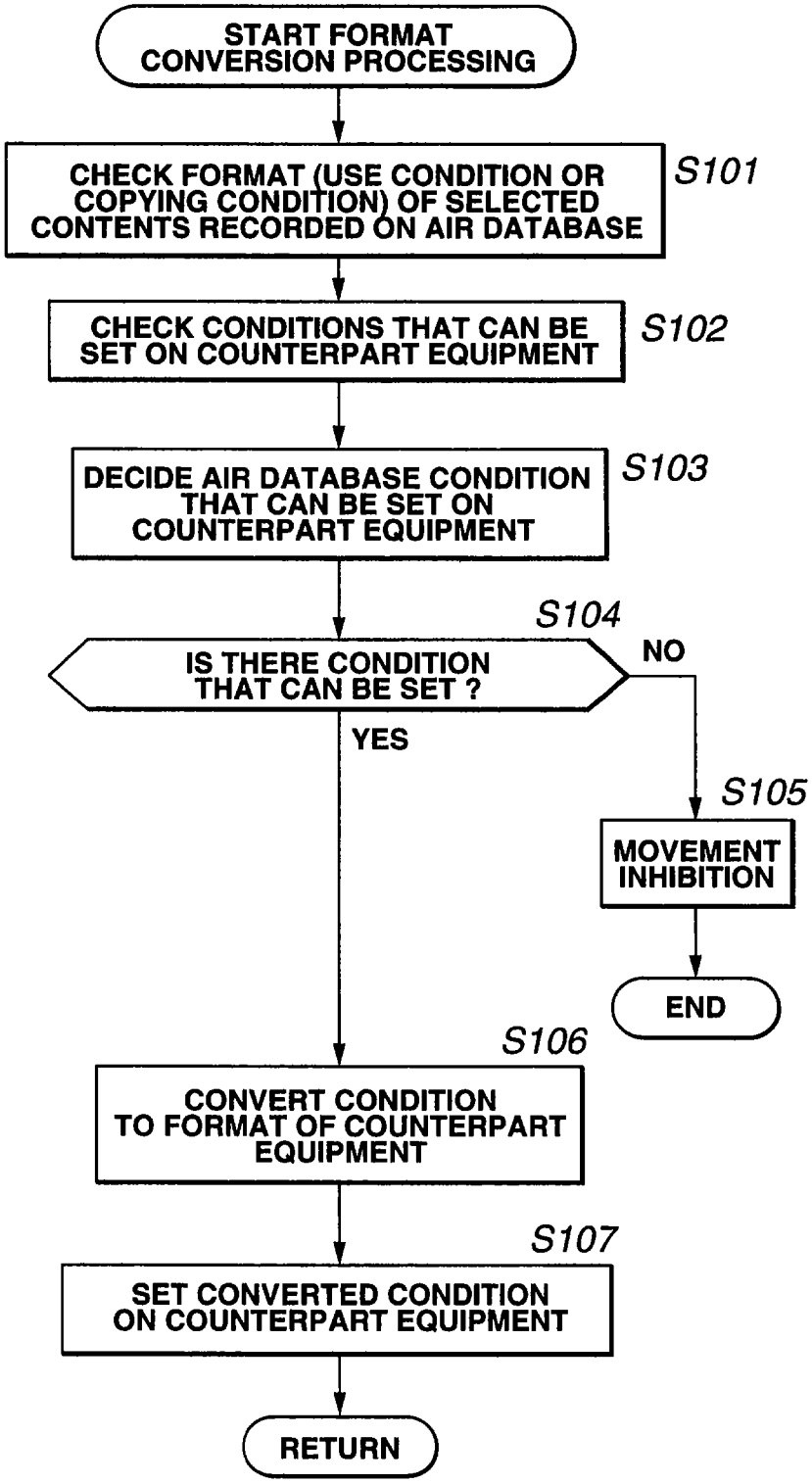

START FORMAT CONVERSION PROCESSING
CHECK FORMAT (USE CONDITION OR COPYING CONDITION) OF SELECTED CONTENTS RECORDED ON AIR DATABASE
S101
CHECK CONDITIONS THAT CAN BE SET ON COUNTERPART EQUIPMENT
S102
DECIDE AIR DATABASE CONDITION THAT CAN BE SET ON COUNTERPART EQUIPMENT
S103
S104
IS THERE CONDITION THAT CAN BE SET ?
NO
YES
S105
MOVEMENT INHIBITION
END
S106
CONVERT CONDITION TO FORMAT OF COUNTERPART EQUIPMENT
S107
SET CONVERTED CONDITION ON COUNTERPART EQUIPMENT
RETURN

FIG.17

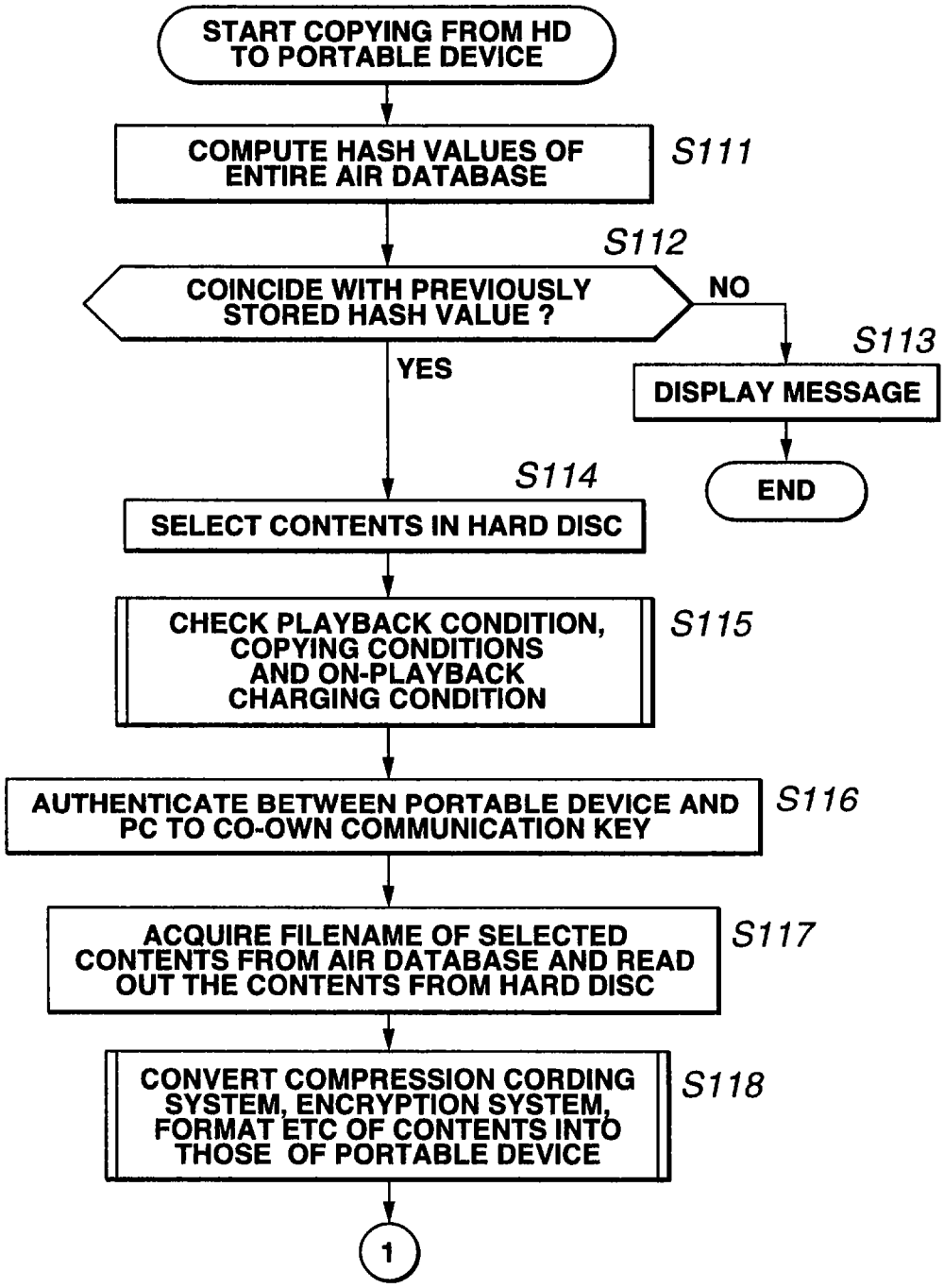

START COPYING FROM HD TO PORTABLE DEVICE
COMPUTE HASH VALUES OF ENTIRE AIR DATABASE
S111
S112
COINCIDE WITH PREVIOUSLY STORED HASH VALUE ?
NO
S113
DISPLAY MESSAGE
END
YES
S114
SELECT CONTENTS IN HARD DISC
CHECK PLAYBACK CONDITION, COPYING CONDITIONS AND ON-PLAYBACK CHARGING CONDITION
S115
AUTHENTICATE BETWEEN PORTABLE DEVICE AND PC TO CO-OWN COMMUNICATION KEY
S116
ACQUIRE FILENAME OF SELECTED CONTENTS FROM AIR DATABASE AND READ OUT THE CONTENTS FROM HARD DISC
S117
CONVERT COMPRESSION CORDING SYSTEM, ENCRYPTION SYSTEM, FORMAT ETC OF CONTENTS INTO THOSE OF PORTABLE DEVICE
S118
1

FIG.18

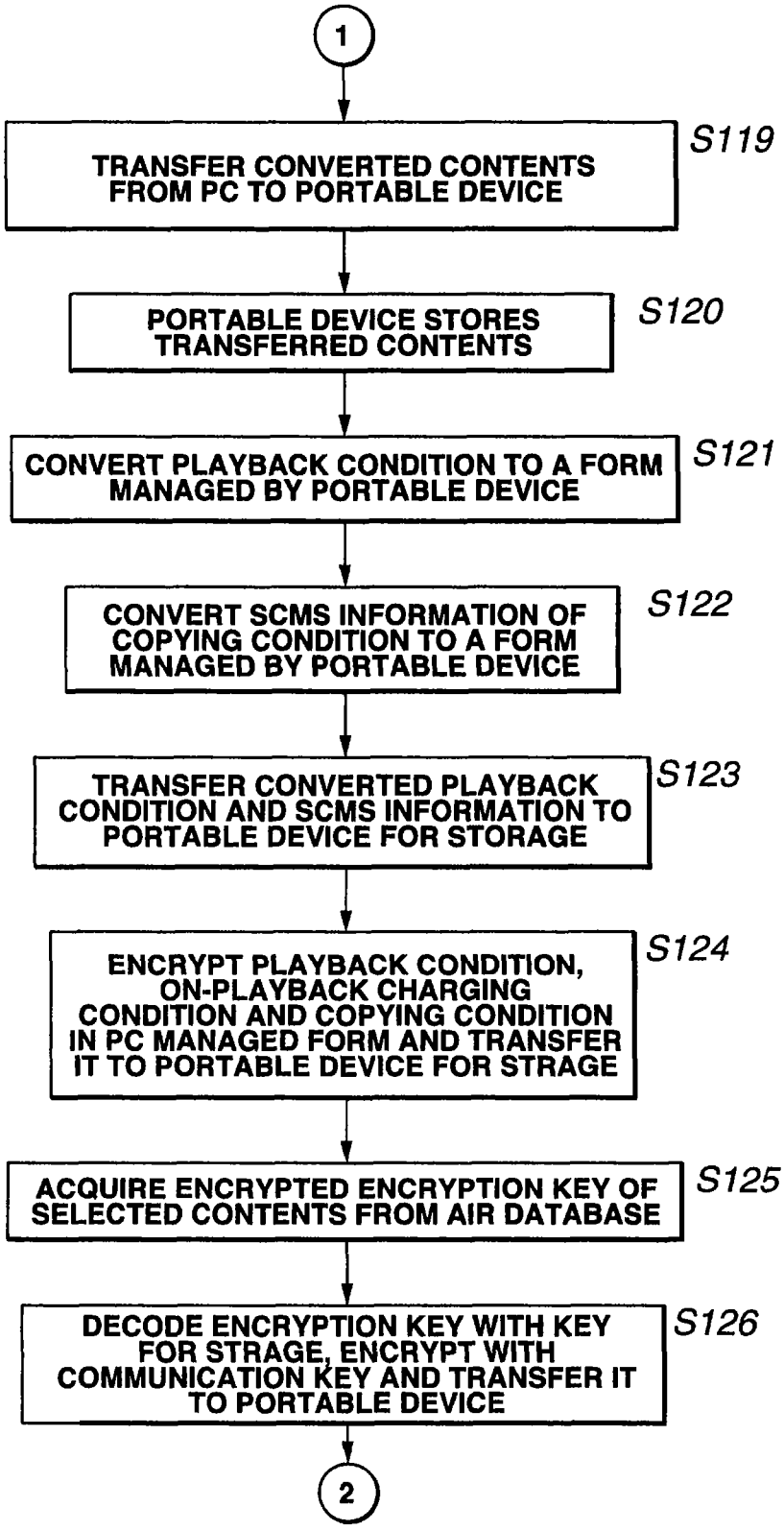

1
TRANSFER CONVERTED CONTENTS FROM PC TO PORTABLE DEVICE
S119
PORTABLE DEVICE STORES TRANSFERRED CONTENTS
S120
CONVERT PLAYBACK CONDITION TO A FORM MANAGED BY PORTABLE DEVICE
S121
CONVERT SCMS INFORMATION OF COPYING CONDITION TO A FORM MANAGED BY PORTABLE DEVICE
S122
TRANSFER CONVERTED PLAYBACK CONDITION AND SCMS INFORMATION TO PORTABLE DEVICE FOR STORAGE
S123
ENCRYPT PLAYBACK CONDITION, ON-PLAYBACK CHARGING CONDITION AND COPYING CONDITION IN PC MANAGED FORM AND TRANSFER IT TO PORTABLE DEVICE FOR STRAGE
S124
ACQUIRE ENCRYPTED ENCRYPTION KEY OF SELECTED CONTENTS FROM AIR DATABASE
S125
DECODE ENCRYPTION KEY WITH KEY FOR STRAGE, ENCRYPT WITH COMMUNICATION KEY AND TRANSFER IT TO PORTABLE DEVICE
S126
2

FIG.19

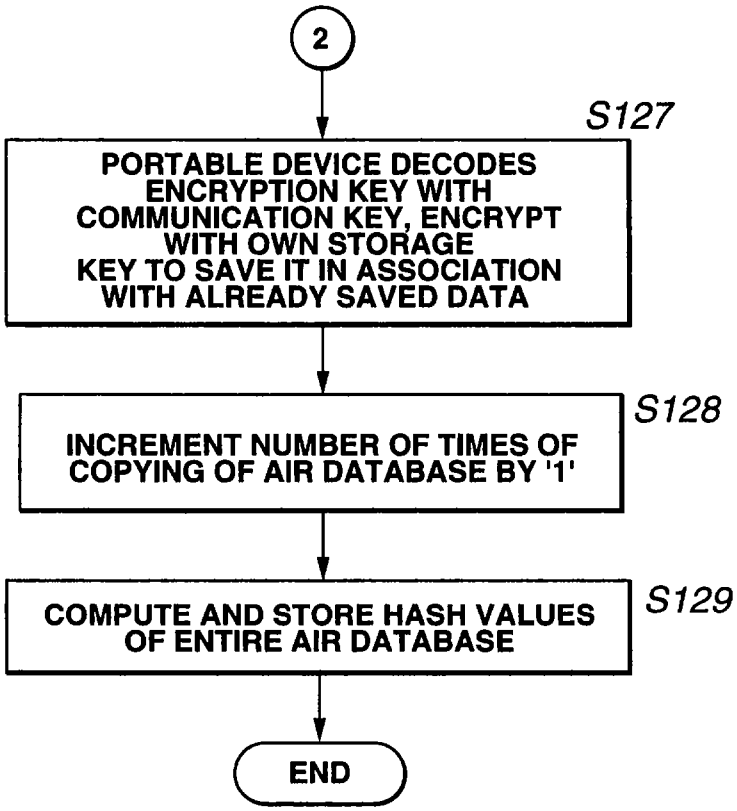

2
S127
PORTABLE DEVICE DECODES ENCRYPTION KEY WITH COMMUNICATION KEY, ENCRYPT WITH OWN STORAGE KEY TO SAVE IT IN ASSOCIATION WITH ALREADY SAVED DATA
S128
INCREMENT NUMBER OF TIMES OF COPYING OF AIR DATABASE BY '1'
S129
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
END

FIG.20

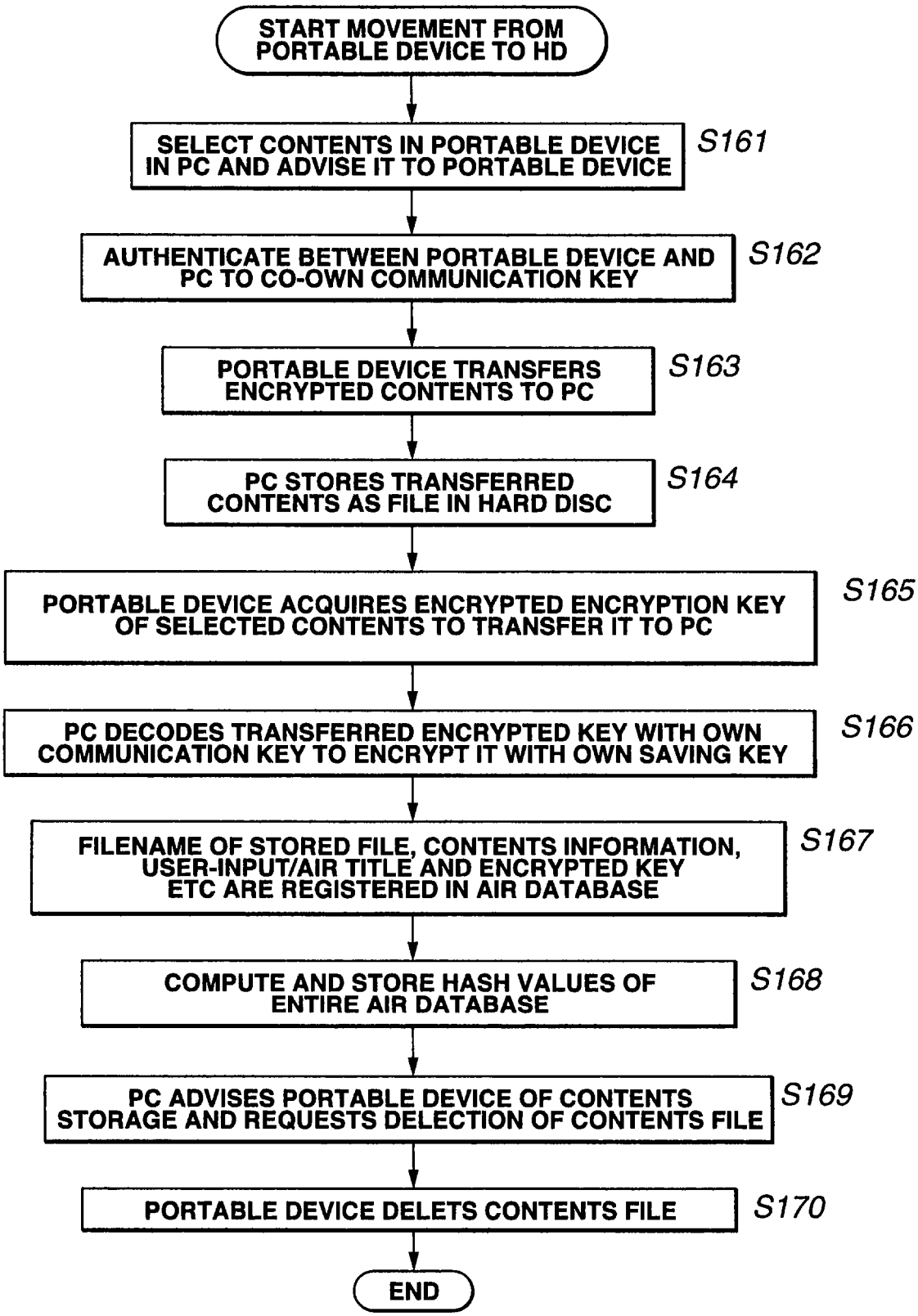

START MOVEMENT FROM PORTABLE DEVICE TO HD
SELECT CONTENTS IN PORTABLE DEVICE IN PC AND ADVISE IT TO PORTABLE DEVICE
S161
AUTHENTICATE BETWEEN PORTABLE DEVICE AND PC TO CO-OWN COMMUNICATION KEY
S162
PORTABLE DEVICE TRANSFERS ENCRYPTED CONTENTS TO PC
S163
PC STORES TRANSFERRED CONTENTS AS FILE IN HARD DISC
S164
PORTABLE DEVICE ACQUIRES ENCRYPTED ENCRYPTION KEY OF SELECTED CONTENTS TO TRANSFER IT TO PC
S165
PC DECODES TRANSFERRED ENCRYPTED KEY WITH OWN COMMUNICATION KEY TO ENCRYPT IT WITH OWN SAVING KEY
S166
FILENAME OF STORED FILE, CONTENTS INFORMATION, USER-INPUT/AIR TITLE AND ENCRYPTED KEY ETC ARE REGISTERED IN AIR DATABASE
S167
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S168
PC ADVISES PORTABLE DEVICE OF CONTENTS STORAGE AND REQUESTS DELECTION OF CONTENTS FILE
S169
PORTABLE DEVICE DELETS CONTENTS FILE
S170
END

FIG.21

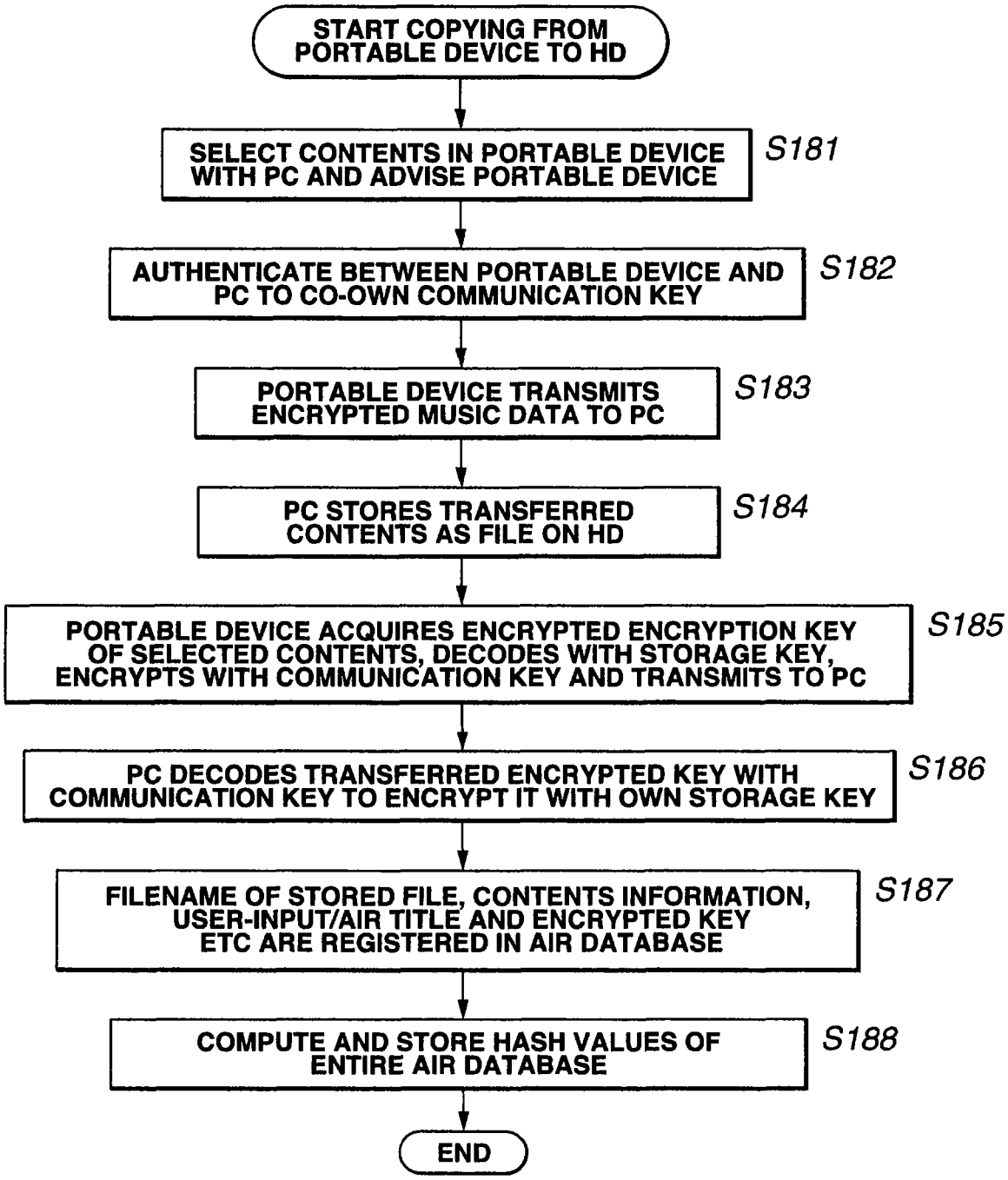

START COPYING FROM PORTABLE DEVICE TO HD
SELECT CONTENTS IN PORTABLE DEVICE WITH PC AND ADVISE PORTABLE DEVICE
S181
AUTHENTICATE BETWEEN PORTABLE DEVICE AND PC TO CO-OWN COMMUNICATION KEY
S182
PORTABLE DEVICE TRANSMITS ENCRYPTED MUSIC DATA TO PC
S183
PC STORES TRANSFERRED CONTENTS AS FILE ON HD
S184
PORTABLE DEVICE ACQUIRES ENCRYPTED ENCRYPTION KEY OF SELECTED CONTENTS, DECODES WITH STORAGE KEY, ENCRYPTS WITH COMMUNICATION KEY AND TRANSMITS TO PC
S185
PC DECODES TRANSFERRED ENCRYPTED KEY WITH COMMUNICATION KEY TO ENCRYPT IT WITH OWN STORAGE KEY
S186
FILENAME OF STORED FILE, CONTENTS INFORMATION, USER-INPUT/AIR TITLE AND ENCRYPTED KEY ETC ARE REGISTERED IN AIR DATABASE
S187
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S188
END

FIG.22

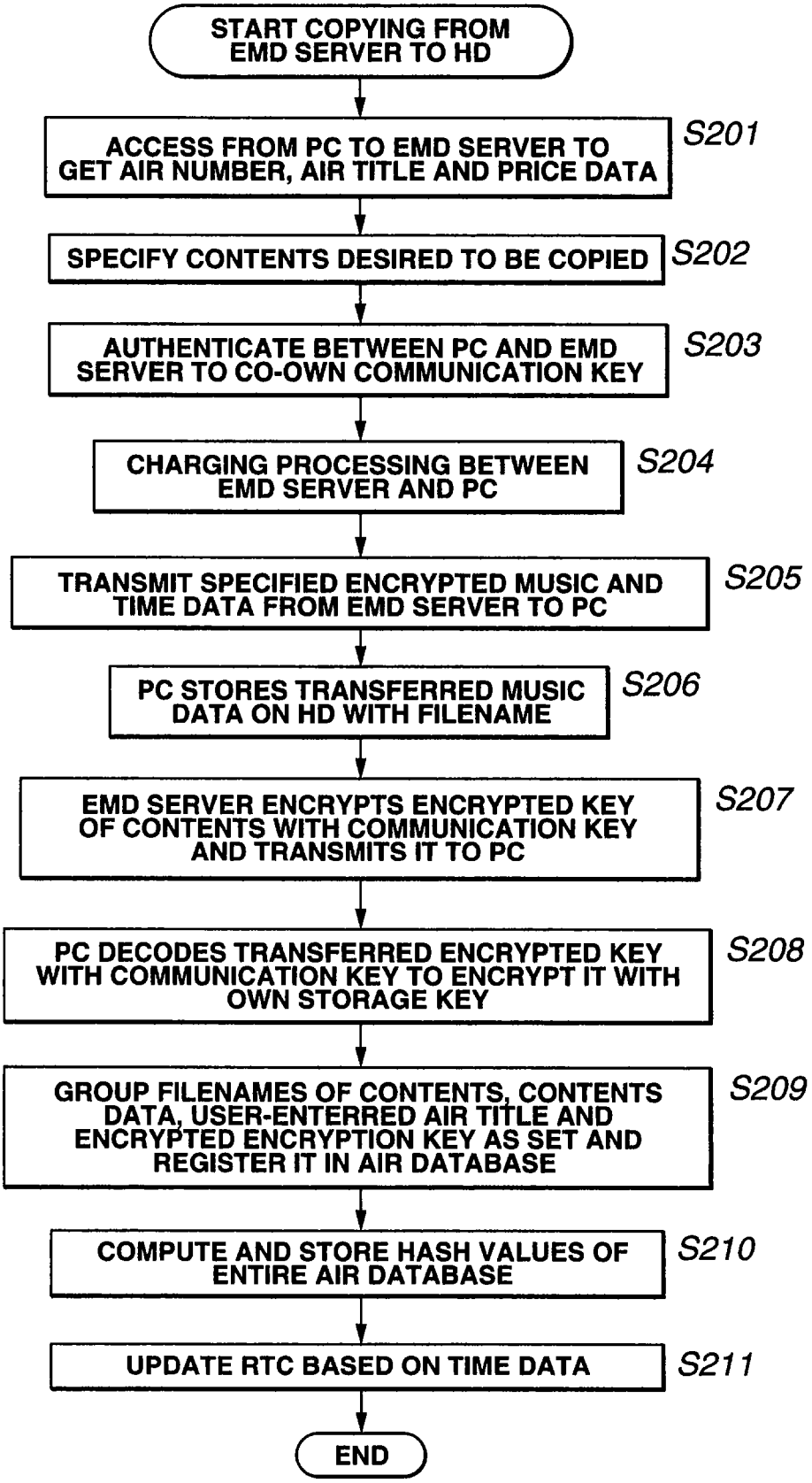

START COPYING FROM EMD SERVER TO HD
ACCESS FROM PC TO EMD SERVER TO GET AIR NUMBER, AIR TITLE AND PRICE DATA
S201
SPECIFY CONTENTS DESIRED TO BE COPIED
S202
AUTHENTICATE BETWEEN PC AND EMD SERVER TO CO-OWN COMMUNICATION KEY
S203
CHARGING PROCESSING BETWEEN EMD SERVER AND PC
S204
TRANSMIT SPECIFIED ENCRYPTED MUSIC AND TIME DATA FROM EMD SERVER TO PC
S205
PC STORES TRANSFERRED MUSIC DATA ON HD WITH FILENAME
S206
EMD SERVER ENCRYPTS ENCRYPTED KEY OF CONTENTS WITH COMMUNICATION KEY AND TRANSMITS IT TO PC
S207
PC DECODES TRANSFERRED ENCRYPTED KEY WITH COMMUNICATION KEY TO ENCRYPT IT WITH OWN STORAGE KEY
S208
GROUP FILENAMES OF CONTENTS, CONTENTS DATA, USER-ENTERRED AIR TITLE AND ENCRYPTED ENCRYPTION KEY AS SET AND REGISTER IT IN AIR DATABASE
S209
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S210
UPDATE RTC BASED ON TIME DATA
S211
END

FIG.23

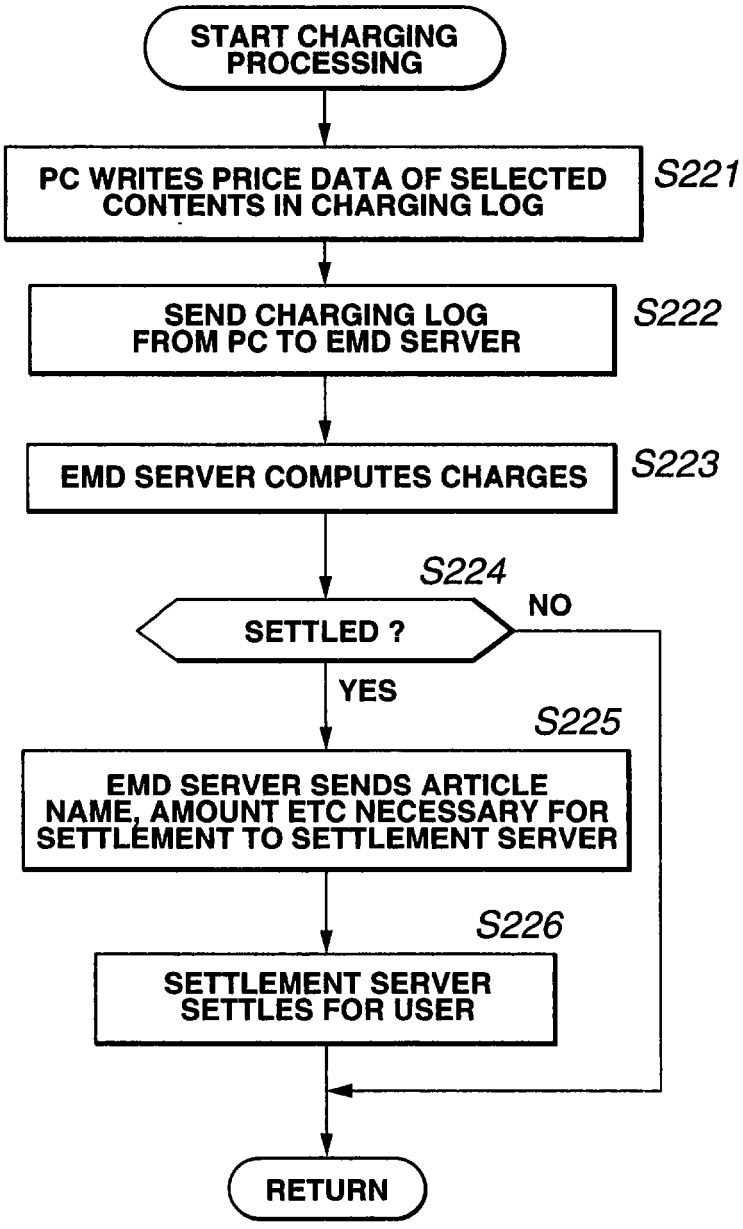

START CHARGING PROCESSING
PC WRITES PRICE DATA OF SELECTED CONTENTS IN CHARGING LOG
S221
SEND CHARGING LOG FROM PC TO EMD SERVER
S222
EMD SERVER COMPUTES CHARGES
S223
S224
SETTLED ?
NO
YES
S225
EMD SERVER SENDS ARTICLE NAME, AMOUNT ETC NECESSARY FOR SETTLEMENT TO SETTLEMENT SERVER
S226
SETTLEMENT SERVER SETTLES FOR USER
RETURN

FIG.24

CHARGING LOG

	ITEM 1	ITEM 2	ITEM 3	
FEE	50	50	60	

HASH VALUE	Oxf8783e263517

FIG.25

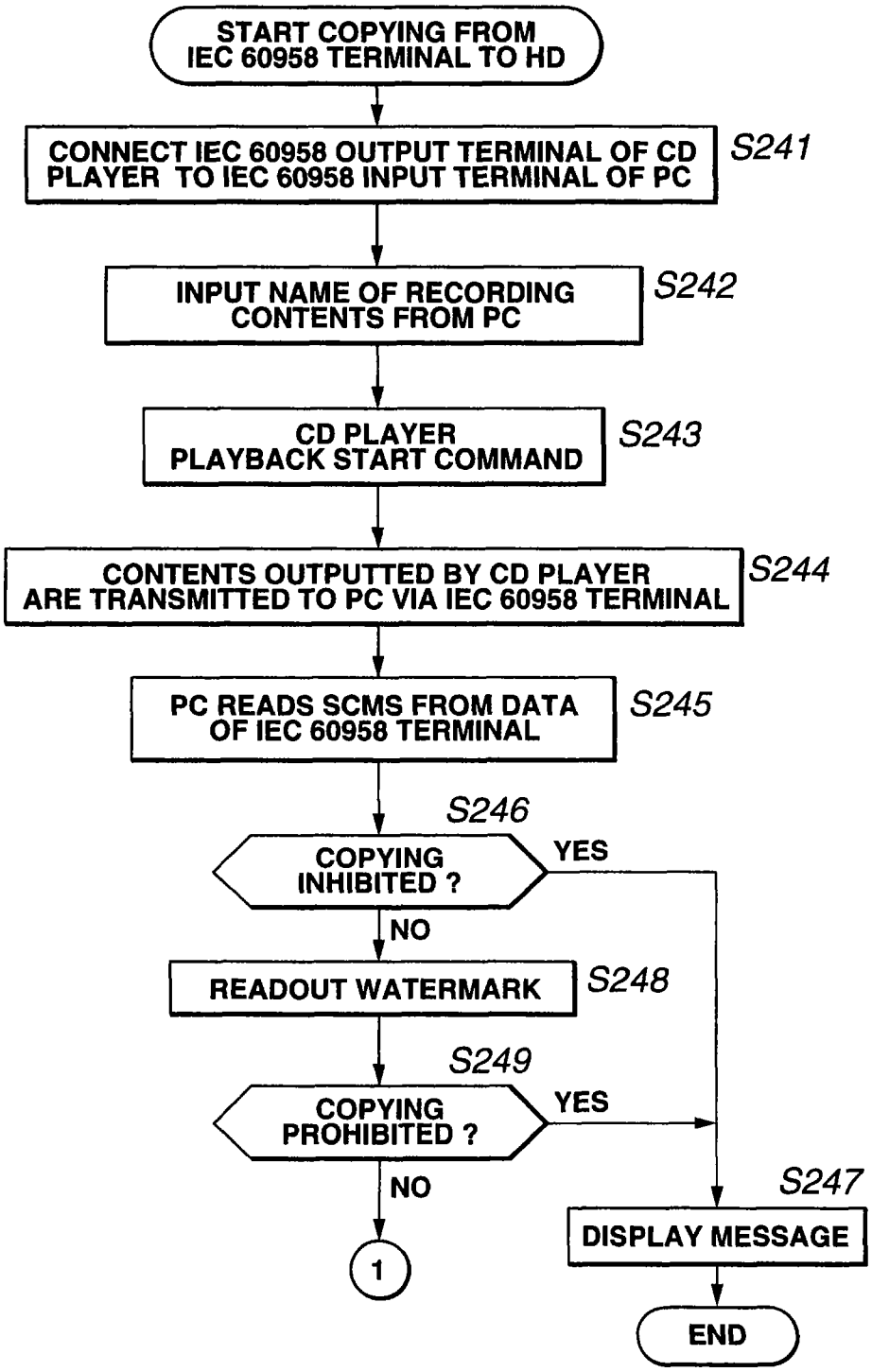

START COPYING FROM IEC 60958 TERMINAL TO HD
CONNECT IEC 60958 OUTPUT TERMINAL OF CD PLAYER TO IEC 60958 INPUT TERMINAL OF PC
S241
INPUT NAME OF RECORDING CONTENTS FROM PC
S242
CD PLAYER PLAYBACK START COMMAND
S243
CONTENTS OUTPUTTED BY CD PLAYER ARE TRANSMITTED TO PC VIA IEC 60958 TERMINAL
S244
PC READS SCMS FROM DATA OF IEC 60958 TERMINAL
S245
S246
COPYING INHIBITED ?
YES
NO
READOUT WATERMARK
S248
S249
COPYING PROHIBITED ?
YES
NO
S247
DISPLAY MESSAGE
1
END

FIG.26

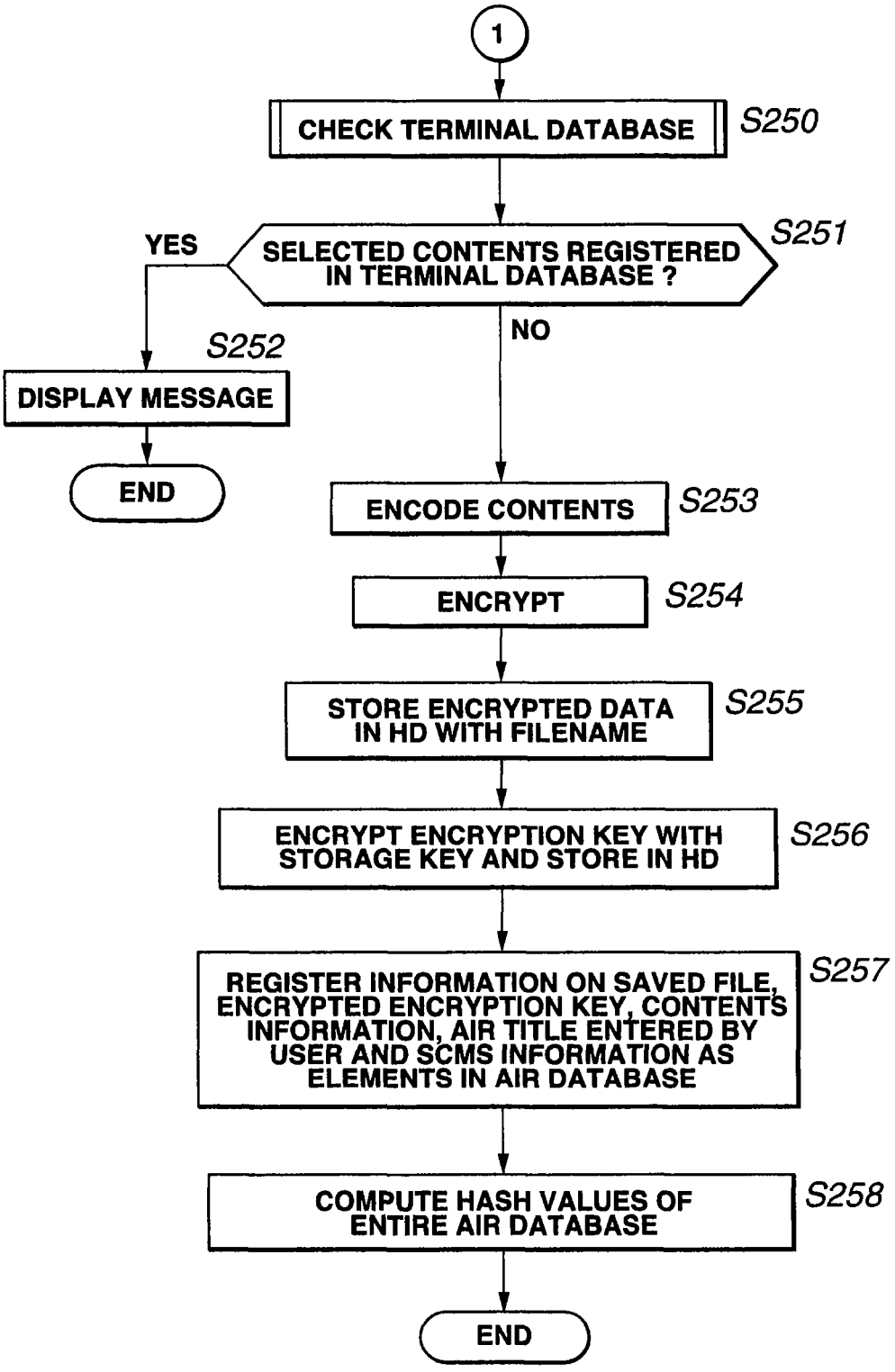

1
CHECK TERMINAL DATABASE
S250
SELECTED CONTENTS REGISTERED IN TERMINAL DATABASE ?
S251
YES
NO
S252
DISPLAY MESSAGE
END
ENCODE CONTENTS
S253
ENCRYPT
S254
STORE ENCRYPTED DATA IN HD WITH FILENAME
S255
ENCRYPT ENCRYPTION KEY WITH STORAGE KEY AND STORE IN HD
S256
REGISTER INFORMATION ON SAVED FILE, ENCRYPTED ENCRYPTION KEY, CONTENTS INFORMATION, AIR TITLE ENTERED BY USER AND SCMS INFORMATION AS ELEMENTS IN AIR DATABASE
S257
COMPUTE HASH VALUES OF ENTIRE AIR DATABASE
S258
END

FIG.27

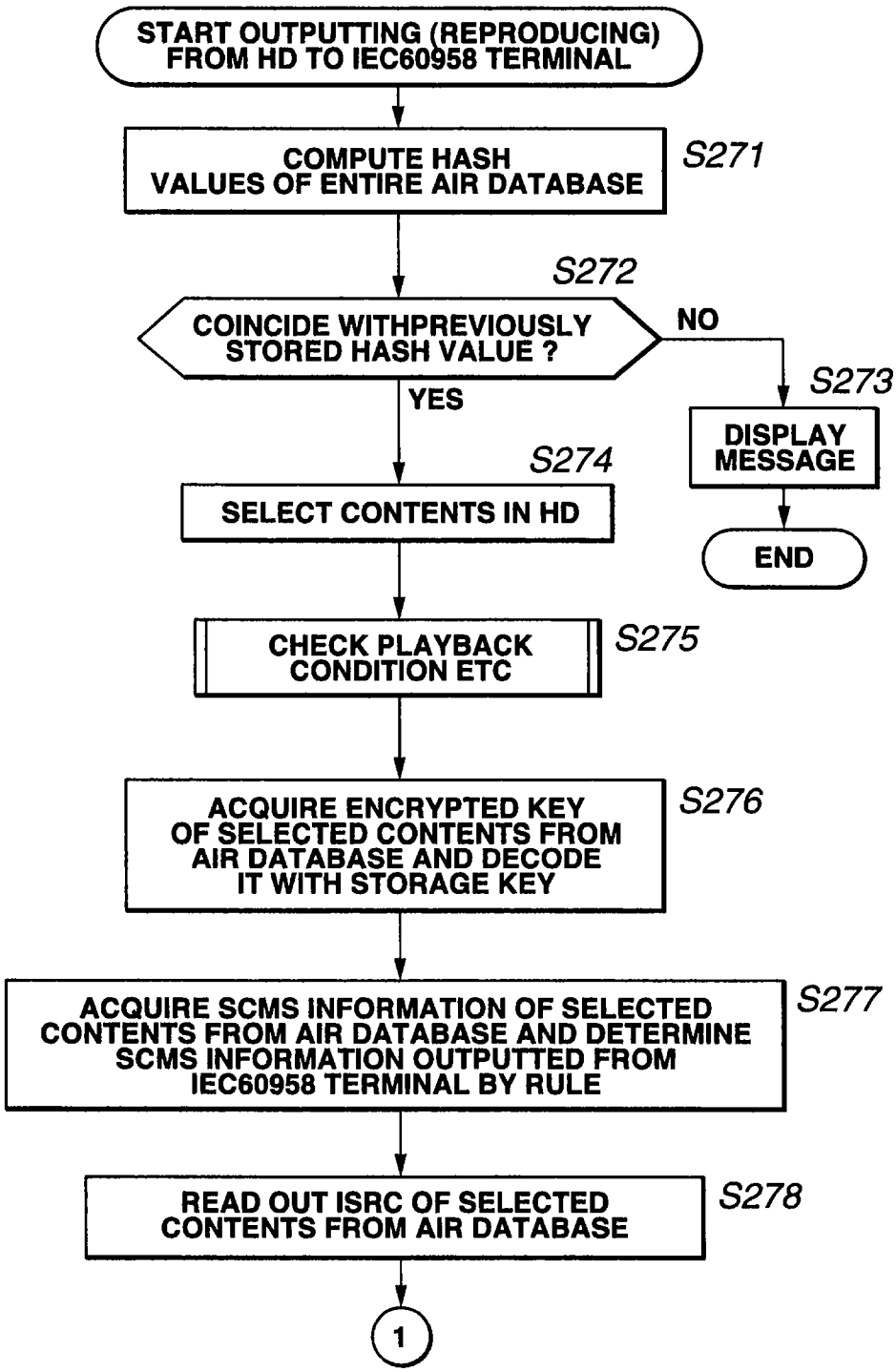

START OUTPUTTING (REPRODUCING) FROM HD TO IEC60958 TERMINAL
COMPUTE HASH VALUES OF ENTIRE AIR DATABASE
S271
S272
COINCIDE WITHPREVIOUSLY STORED HASH VALUE ?
NO
YES
S273
DISPLAY MESSAGE
END
S274
SELECT CONTENTS IN HD
CHECK PLAYBACK CONDITION ETC
S275
ACQUIRE ENCRYPTED KEY OF SELECTED CONTENTS FROM AIR DATABASE AND DECODE IT WITH STORAGE KEY
S276
ACQUIRE SCMS INFORMATION OF SELECTED CONTENTS FROM AIR DATABASE AND DETERMINE SCMS INFORMATION OUTPUTTED FROM IEC60958 TERMINAL BY RULE
S277
READ OUT ISRC OF SELECTED CONTENTS FROM AIR DATABASE
S278
1

FIG.28

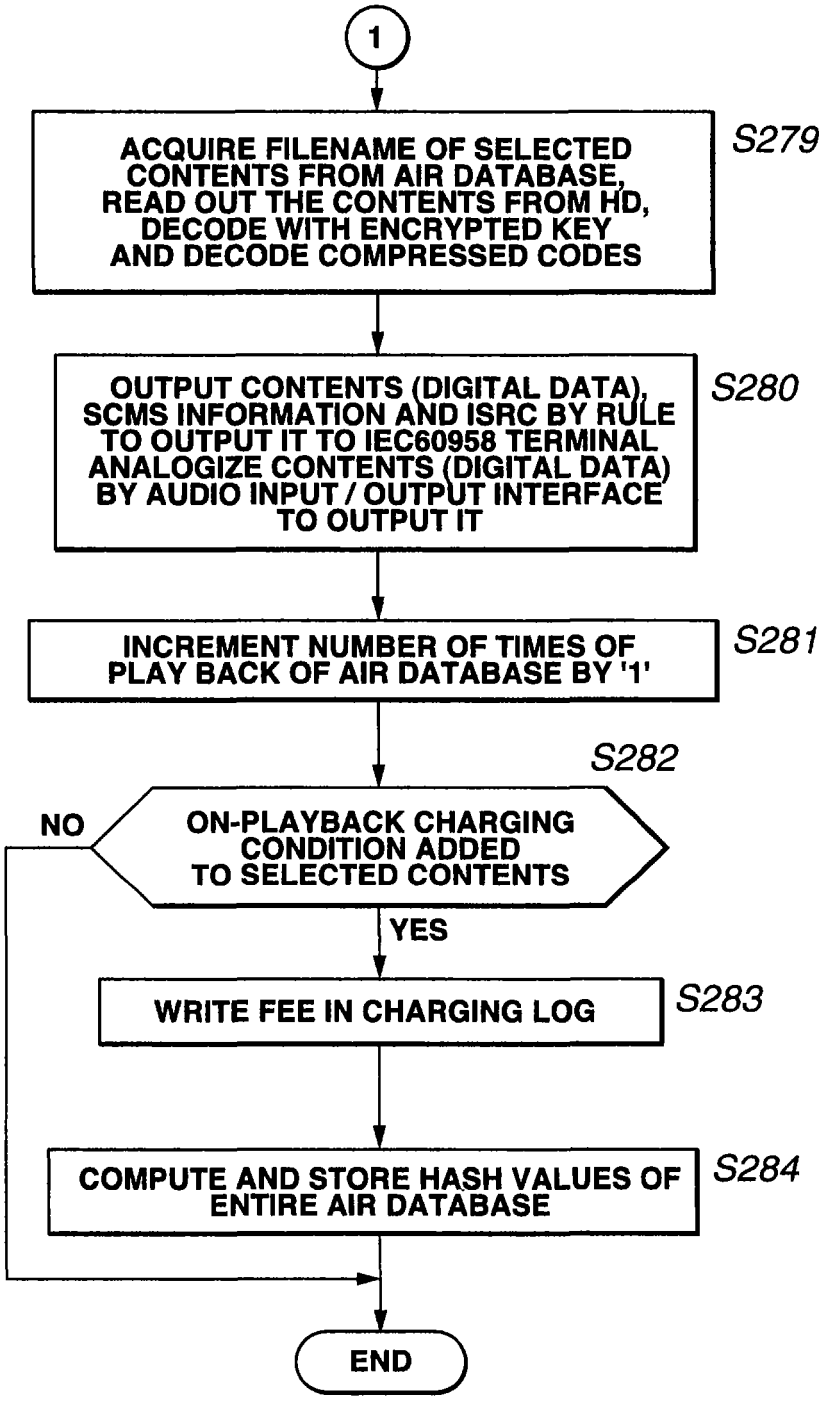

1
ACQUIRE FILENAME OF SELECTED CONTENTS FROM AIR DATABASE, READ OUT THE CONTENTS FROM HD, DECODE WITH ENCRYPTED KEY AND DECODE COMPRESSED CODES
S279
OUTPUT CONTENTS (DIGITAL DATA), SCMS INFORMATION AND ISRC BY RULE TO OUTPUT IT TO IEC60958 TERMINAL ANALOGIZE CONTENTS (DIGITAL DATA) BY AUDIO INPUT / OUTPUT INTERFACE TO OUTPUT IT
S280
INCREMENT NUMBER OF TIMES OF PLAY BACK OF AIR DATABASE BY '1'
S281
S282
NO
ON-PLAYBACK CHARGING CONDITION ADDED TO SELECTED CONTENTS
YES
WRITE FEE IN CHARGING LOG
S283
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S284
END

FIG.29

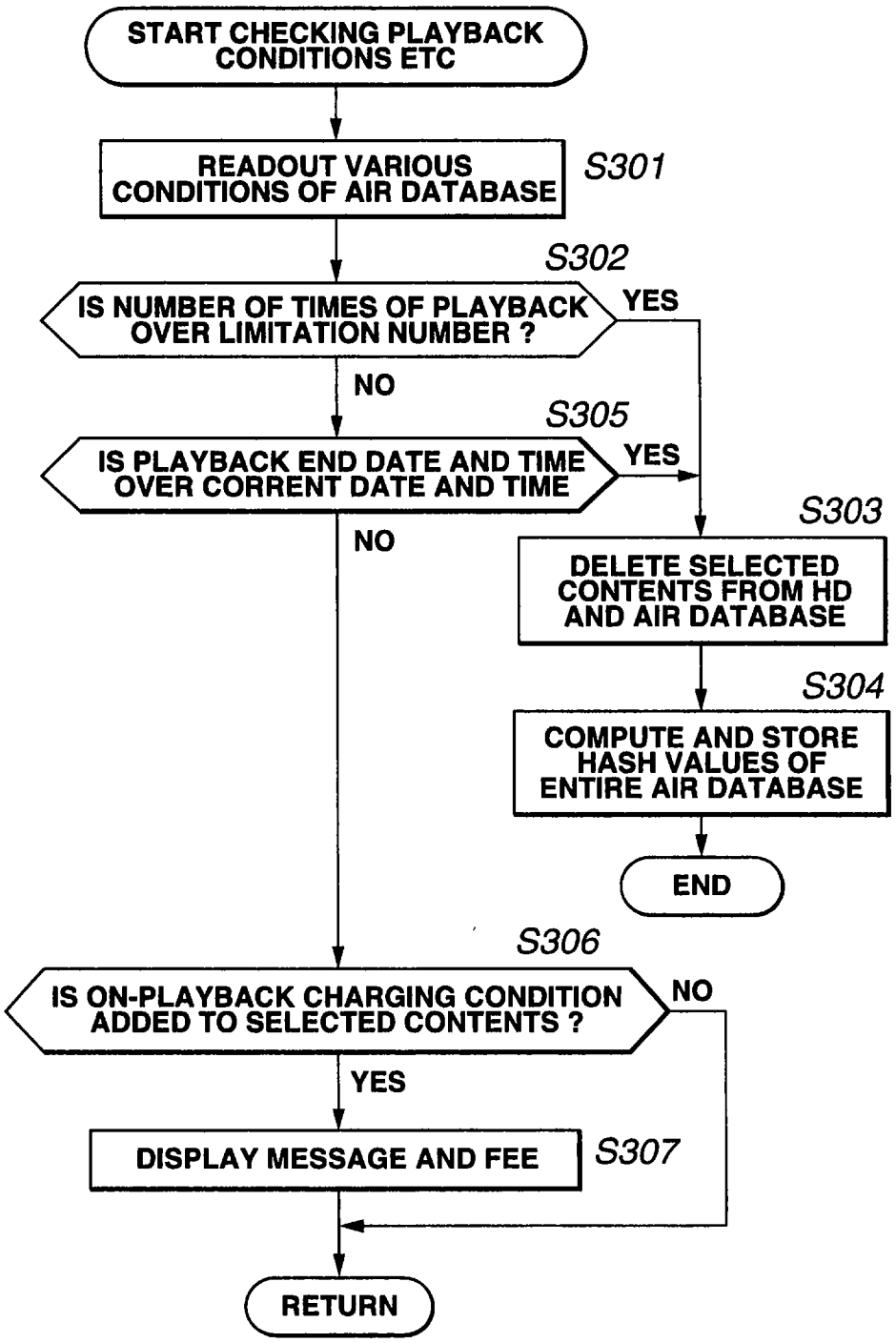

START CHECKING PLAYBACK CONDITIONS ETC
READOUT VARIOUS CONDITIONS OF AIR DATABASE
S301
S302
IS NUMBER OF TIMES OF PLAYBACK OVER LIMITATION NUMBER ?
YES
NO
S305
IS PLAYBACK END DATE AND TIME OVER CORRENT DATE AND TIME
YES
NO
S303
DELETE SELECTED CONTENTS FROM HD AND AIR DATABASE
S304
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
END
S306
IS ON-PLAYBACK CHARGING CONDITION ADDED TO SELECTED CONTENTS ?
NO
YES
DISPLAY MESSAGE AND FEE
S307
RETURN

FIG.30

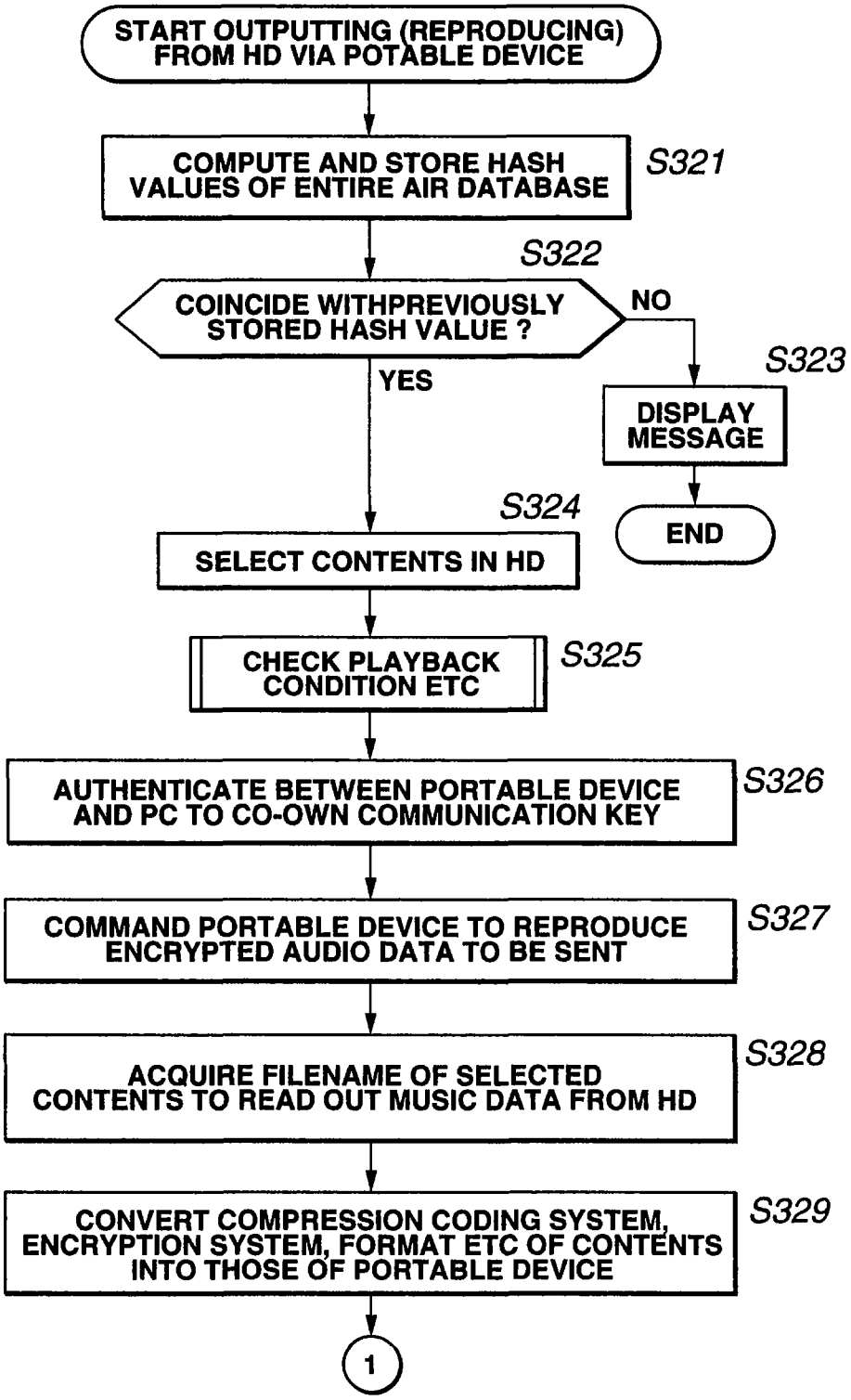

START OUTPUTTING (REPRODUCING) FROM HD VIA POTABLE DEVICE
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S321
S322
COINCIDE WITHPREVIOUSLY STORED HASH VALUE ?
NO
S323
YES
DISPLAY MESSAGE
END
S324
SELECT CONTENTS IN HD
CHECK PLAYBACK CONDITION ETC
S325
AUTHENTICATE BETWEEN PORTABLE DEVICE AND PC TO CO-OWN COMMUNICATION KEY
S326
COMMAND PORTABLE DEVICE TO REPRODUCE ENCRYPTED AUDIO DATA TO BE SENT
S327
ACQUIRE FILENAME OF SELECTED CONTENTS TO READ OUT MUSIC DATA FROM HD
S328
CONVERT COMPRESSION CODING SYSTEM, ENCRYPTION SYSTEM, FORMAT ETC OF CONTENTS INTO THOSE OF PORTABLE DEVICE
S329
1

FIG.31

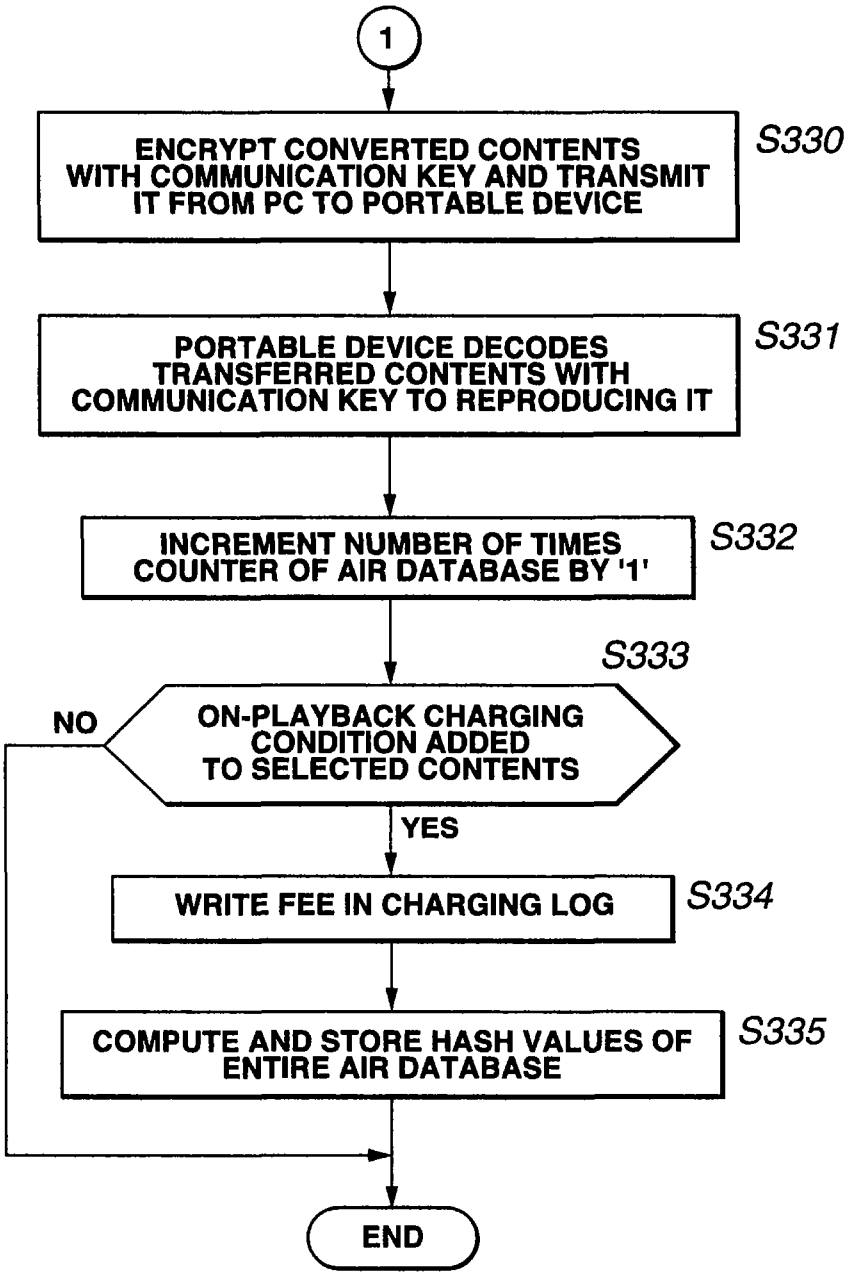

1
ENCRYPT CONVERTED CONTENTS WITH COMMUNICATION KEY AND TRANSMIT IT FROM PC TO PORTABLE DEVICE
S330
PORTABLE DEVICE DECODES TRANSFERRED CONTENTS WITH COMMUNICATION KEY TO REPRODUCING IT
S331
INCREMENT NUMBER OF TIMES COUNTER OF AIR DATABASE BY '1'
S332
S333
NO
ON-PLAYBACK CHARGING CONDITION ADDED TO SELECTED CONTENTS
YES
WRITE FEE IN CHARGING LOG
S334
COMPUTE AND STORE HASH VALUES OF ENTIRE AIR DATABASE
S335
END

FIG.32

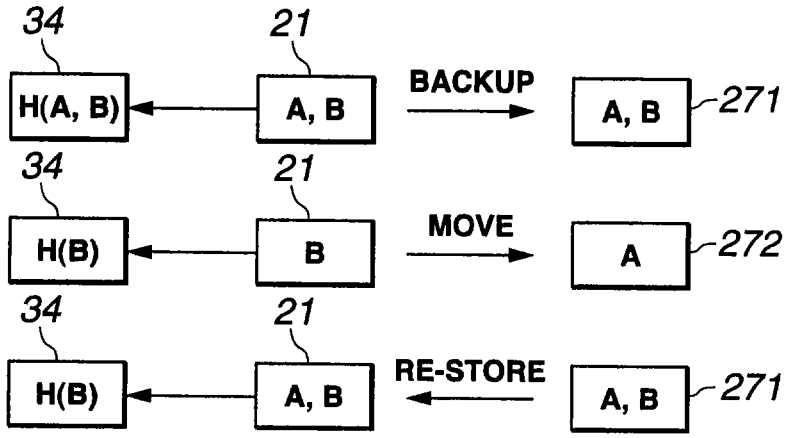

34
21
H(A, B)
A, B
BACKUP
A, B
271
34
21
H(B)
B
MOVE
A
272
34
21
H(B)
A, B
RE-STORE
A, B
271

FIG.33

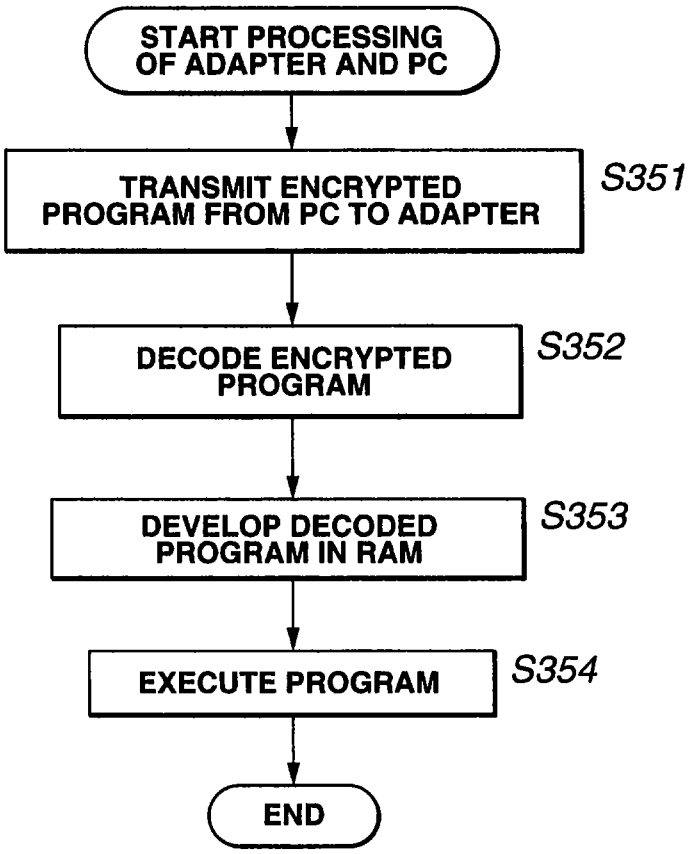

START PROCESSING OF ADAPTER AND PC
TRANSMIT ENCRYPTED PROGRAM FROM PC TO ADAPTER
S351
DECODE ENCRYPTED PROGRAM
S352
DEVELOP DECODED PROGRAM IN RAM
S353
EXECUTE PROGRAM
S354
END

FIG.34

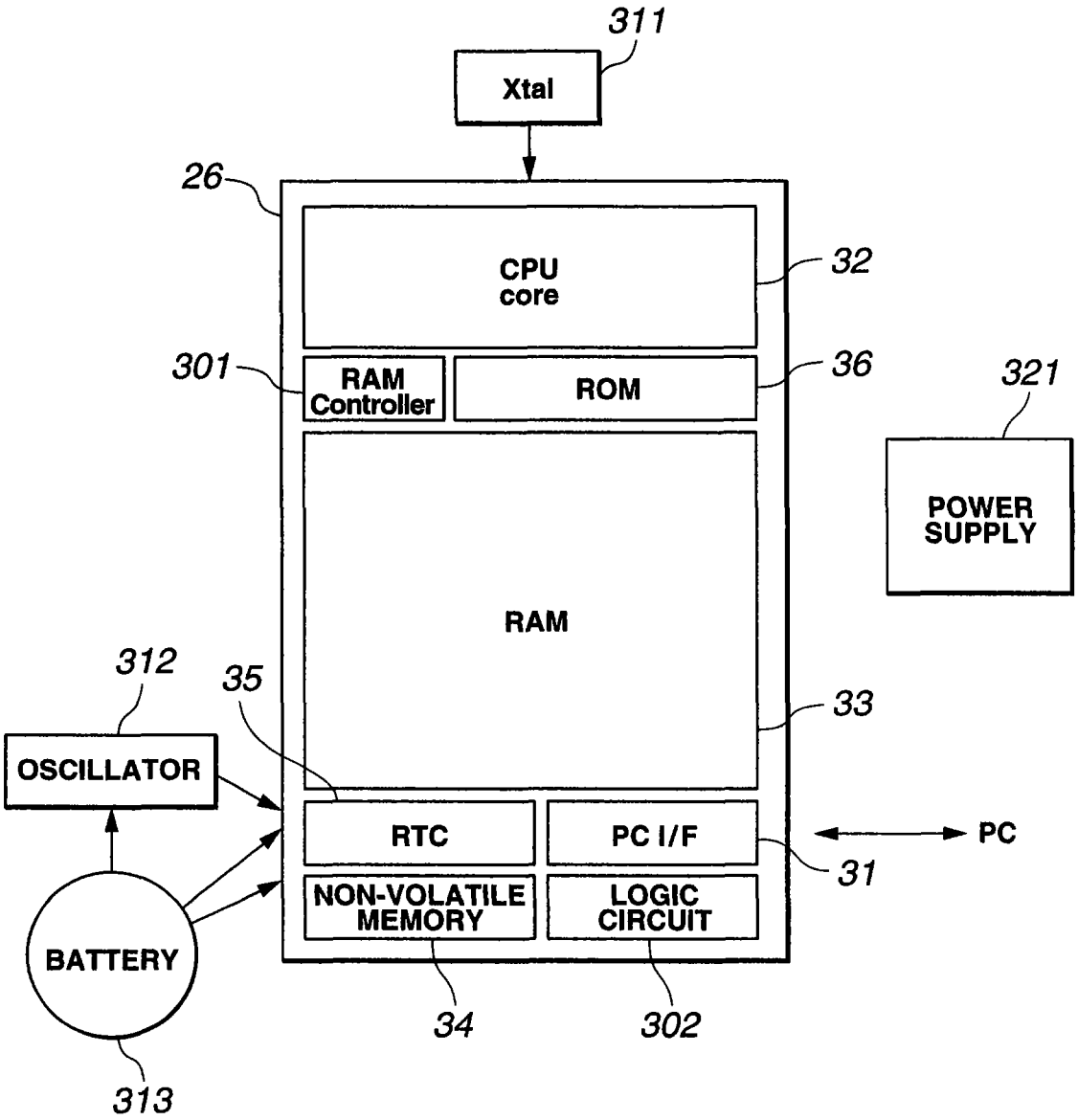

311
Xtal
26
CPU
core
32
301
RAM
Controller
ROM
36
321
POWER
SUPPLY
RAM
312
35
33
OSCILLATOR
RTC
PC I/F
PC
31
NON-VOLATILE
MEMORY
LOGIC
CIRCUIT
BATTERY
34
302
313

FIG.35

FIG.36A

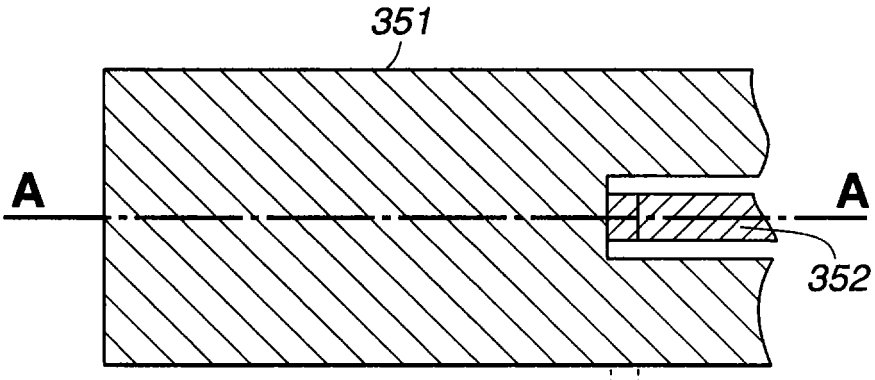
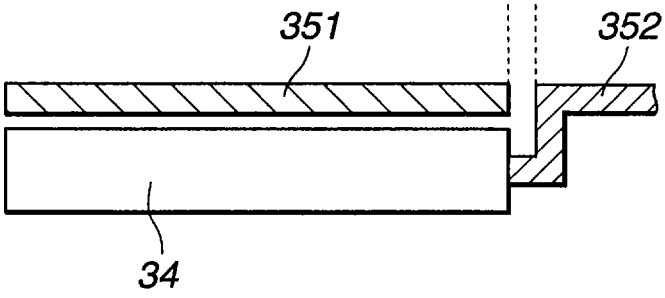


FIG.36B



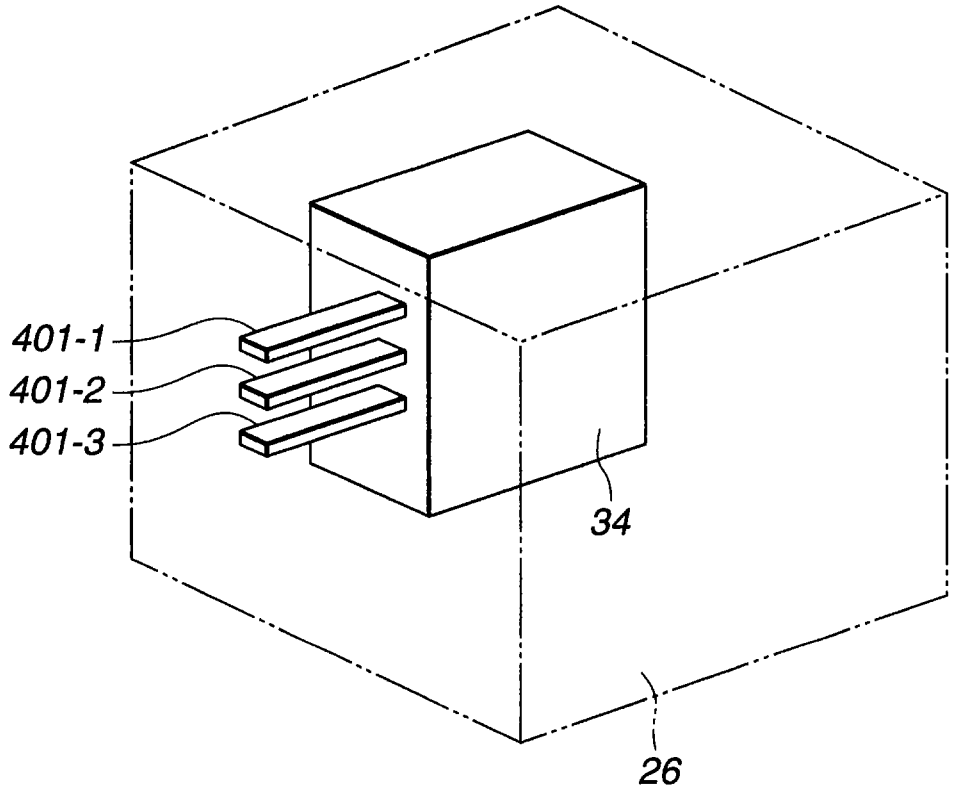


FIG.37

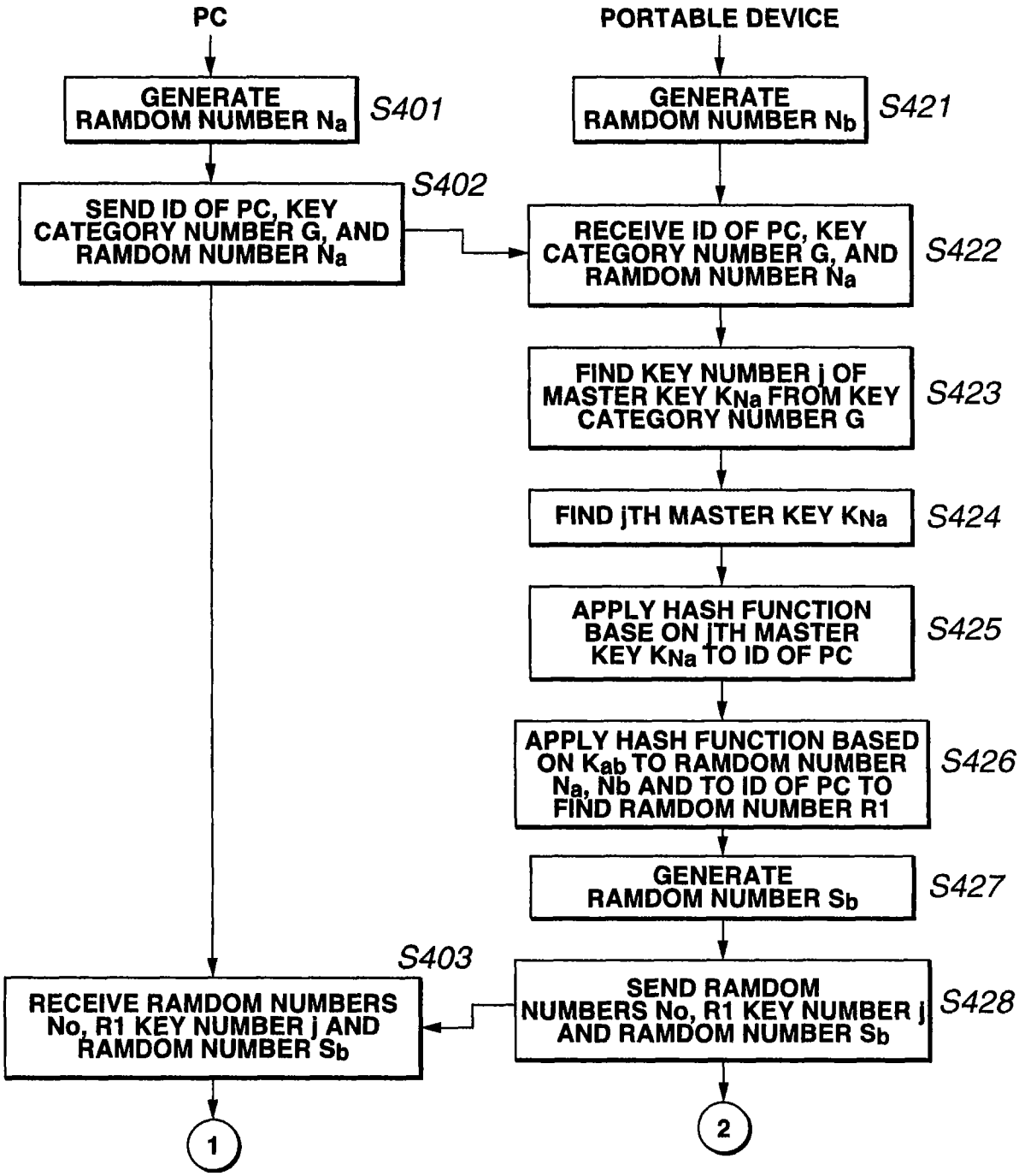

PC
PORTABLE DEVICE
GENERATE RAMDOM NUMBER Na
S401
GENERATE RAMDOM NUMBER Nb
S421
SEND ID OF PC, KEY CATEGORY NUMBER G, AND RAMDOM NUMBER Na
S402
RECEIVE ID OF PC, KEY CATEGORY NUMBER G, AND RAMDOM NUMBER Na
S422
FIND KEY NUMBER j OF MASTER KEY KNa FROM KEY CATEGORY NUMBER G
S423
FIND jTH MASTER KEY KNa
S424
APPLY HASH FUNCTION BASE ON jTH MASTER KEY KNa TO ID OF PC
S425
APPLY HASH FUNCTION BASED ON Kab TO RAMDOM NUMBER Na, Nb AND TO ID OF PC TO FIND RAMDOM NUMBER R1
S426
GENERATE RAMDOM NUMBER Sb
S427
S403
RECEIVE RAMDOM NUMBERS No, R1 KEY NUMBER j AND RAMDOM NUMBER Sb
SEND RAMDOM NUMBERS No, R1 KEY NUMBER j AND RAMDOM NUMBER Sb
S428
1
2

FIG.38

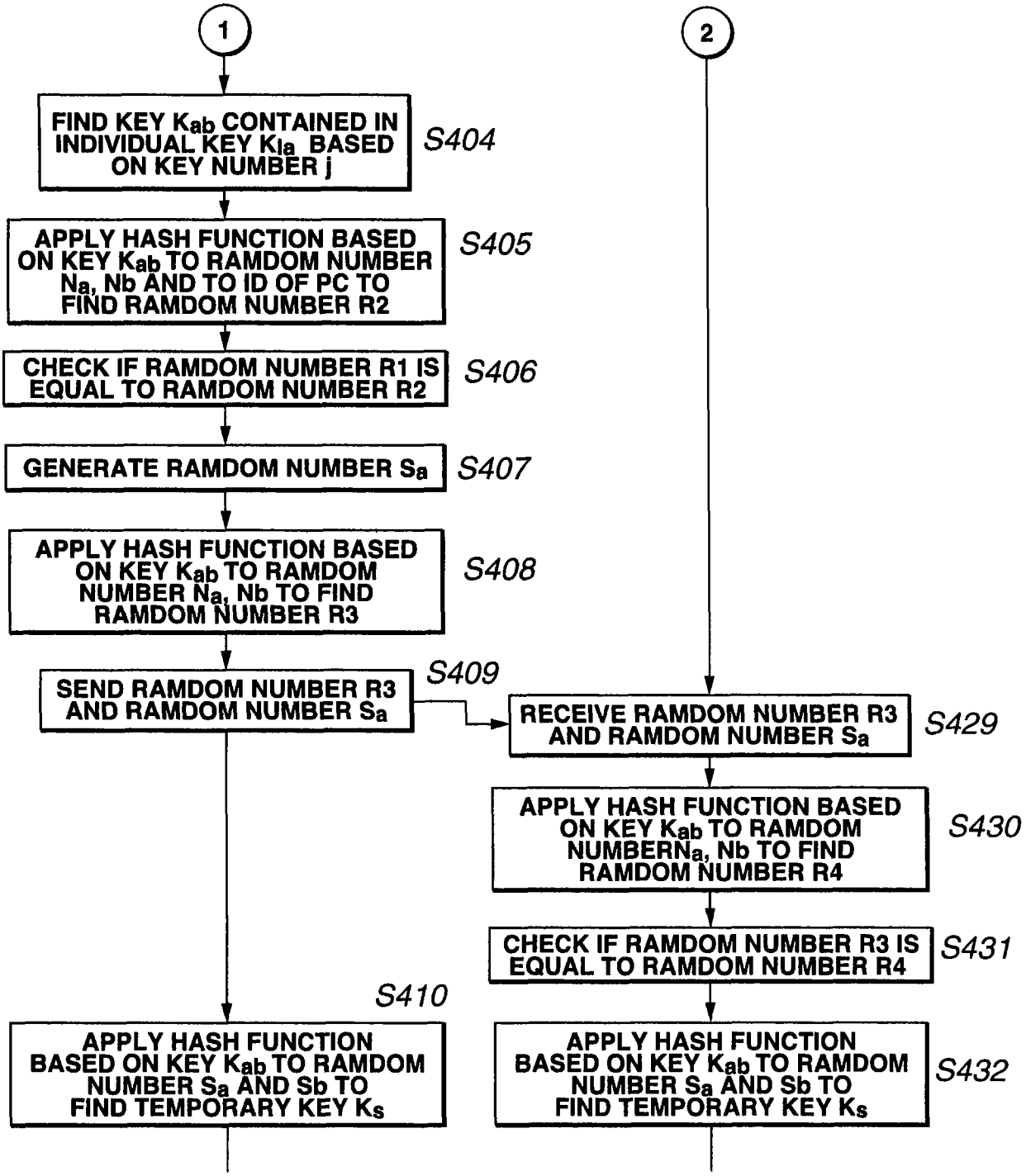

1
2
FIND KEY Kab CONTAINED IN INDIVIDUAL KEY Kia BASED ON KEY NUMBER j
S404
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBER Na, Nb AND TO ID OF PC TO FIND RAMDOM NUMBER R2
S405
CHECK IF RAMDOM NUMBER R1 IS EQUAL TO RAMDOM NUMBER R2
S406
GENERATE RAMDOM NUMBER Sa
S407
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBER Na, Nb TO FIND RAMDOM NUMBER R3
S408
SEND RAMDOM NUMBER R3 AND RAMDOM NUMBER Sa
S409
RECEIVE RAMDOM NUMBER R3 AND RAMDOM NUMBER Sa
S429
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBERNa, Nb TO FIND RAMDOM NUMBER R4
S430
CHECK IF RAMDOM NUMBER R3 IS EQUAL TO RAMDOM NUMBER R4
S431
S410
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBER Sa AND Sb TO FIND TEMPORARY KEY Ks
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBER Sa AND Sb TO FIND TEMPORARY KEY Ks
S432

FIG.39

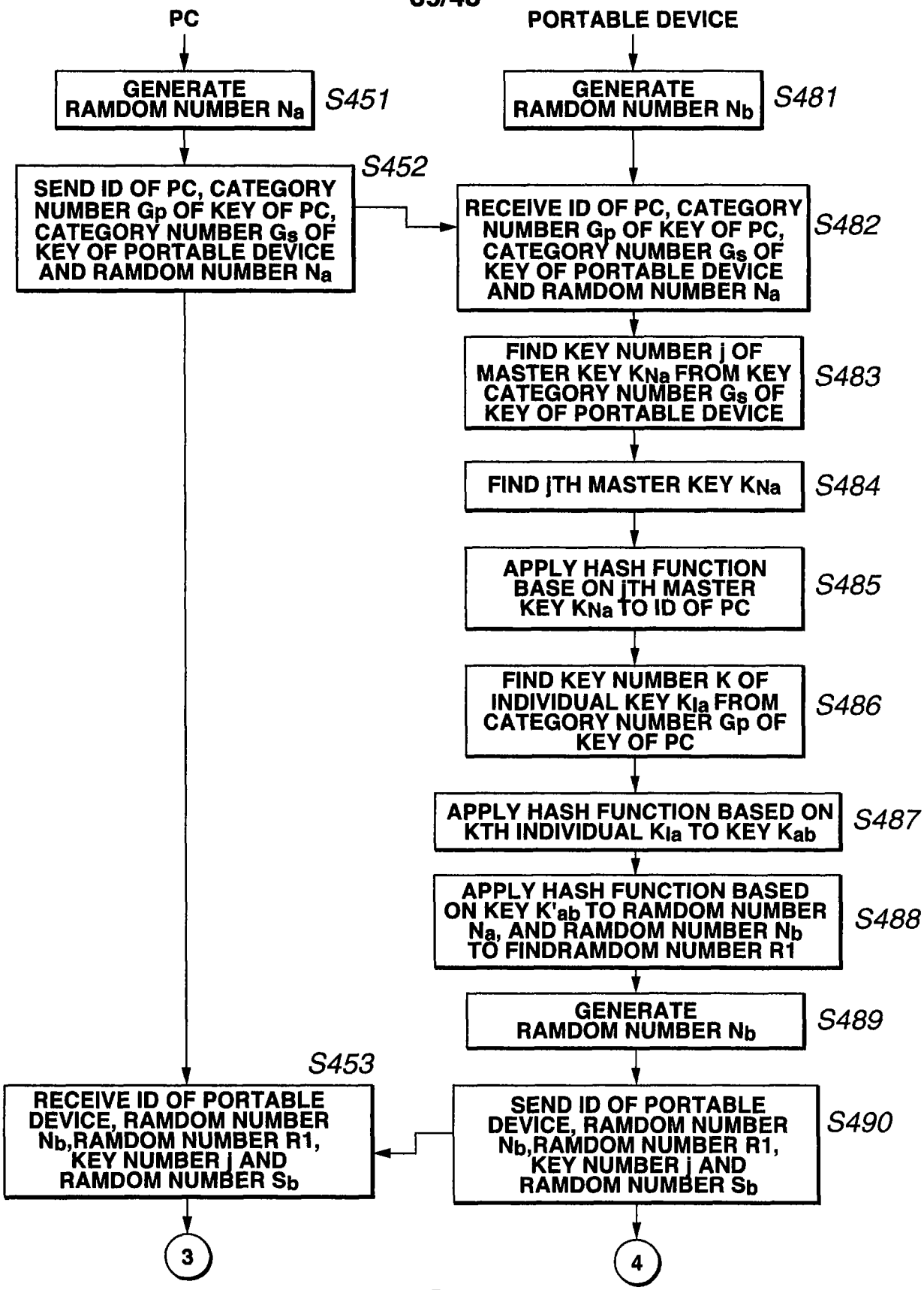

PC
PORTABLE DEVICE
GENERATE RAMDOM NUMBER Na
S451
GENERATE RAMDOM NUMBER Nb
S481
S452
SEND ID OF PC, CATEGORY NUMBER Gp OF KEY OF PC, CATEGORY NUMBER Gs OF KEY OF PORTABLE DEVICE AND RAMDOM NUMBER Na
RECEIVE ID OF PC, CATEGORY NUMBER Gp OF KEY OF PC, CATEGORY NUMBER Gs OF KEY OF PORTABLE DEVICE AND RAMDOM NUMBER Na
S482
FIND KEY NUMBER j OF MASTER KEY KNa FROM KEY CATEGORY NUMBER Gs OF KEY OF PORTABLE DEVICE
S483
FIND jTH MASTER KEY KNa
S484
APPLY HASH FUNCTION BASE ON jTH MASTER KEY KNa TO ID OF PC
S485
FIND KEY NUMBER K OF INDIVIDUAL KEY Kla FROM CATEGORY NUMBER Gp OF KEY OF PC
S486
APPLY HASH FUNCTION BASED ON KTH INDIVIDUAL Kla TO KEY Kab
S487
APPLY HASH FUNCTION BASED ON KEY K'ab TO RAMDOM NUMBER Na, AND RAMDOM NUMBER Nb TO FINDRAMDOM NUMBER R1
S488
GENERATE RAMDOM NUMBER Nb
S489
S453
RECEIVE ID OF PORTABLE DEVICE, RAMDOM NUMBER Nb,RAMDOM NUMBER R1, KEY NUMBER j AND RAMDOM NUMBER Sb
SEND ID OF PORTABLE DEVICE, RAMDOM NUMBER Nb,RAMDOM NUMBER R1, KEY NUMBER j AND RAMDOM NUMBER Sb
S490
3
4

FIG.40

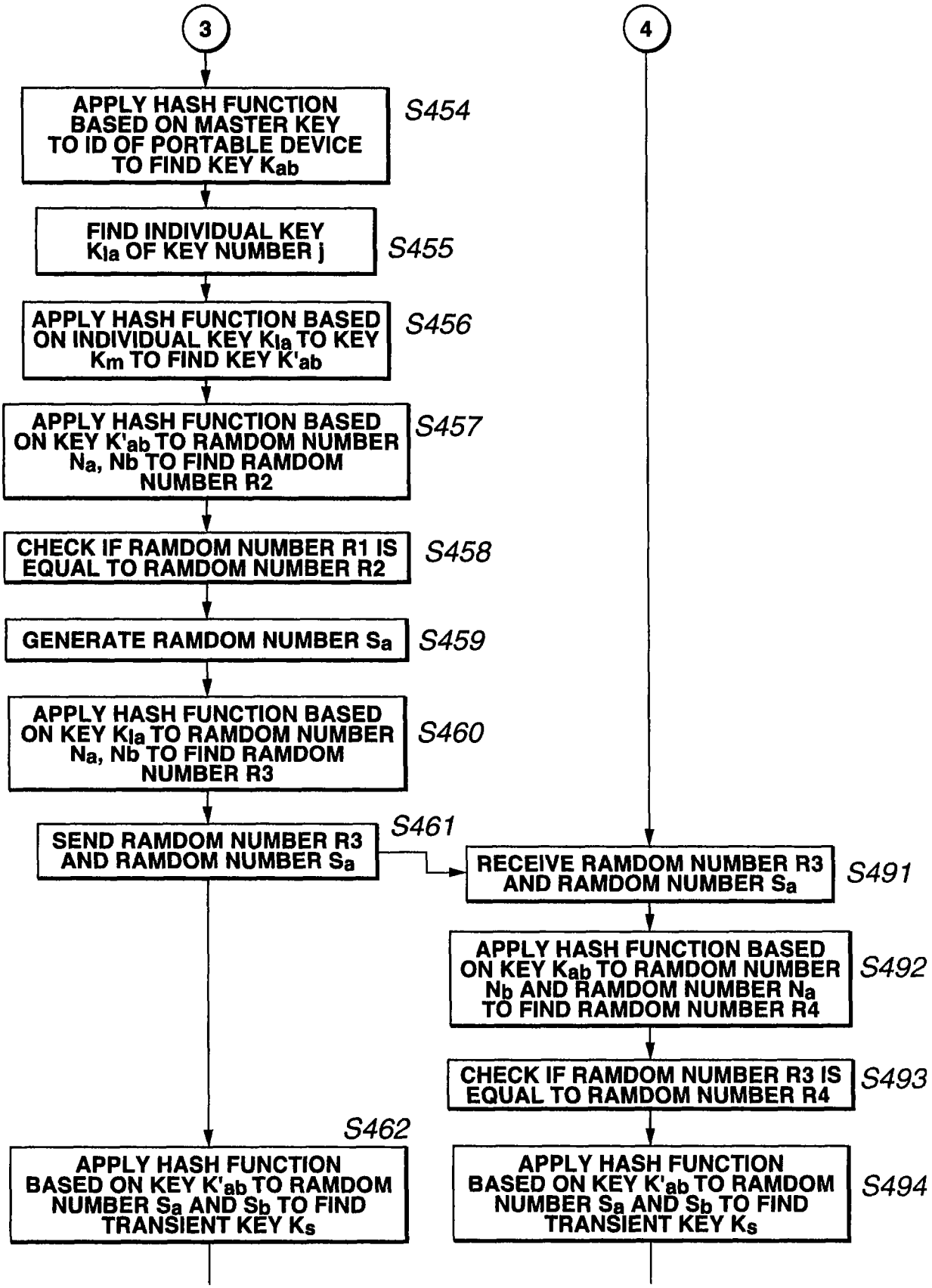

3
4
APPLY HASH FUNCTION BASED ON MASTER KEY TO ID OF PORTABLE DEVICE TO FIND KEY Kab
S454
FIND INDIVIDUAL KEY Kla OF KEY NUMBER j
S455
APPLY HASH FUNCTION BASED ON INDIVIDUAL KEY Kla TO KEY Km TO FIND KEY K'ab
S456
APPLY HASH FUNCTION BASED ON KEY K'ab TO RAMDOM NUMBER Na, Nb TO FIND RAMDOM NUMBER R2
S457
CHECK IF RAMDOM NUMBER R1 IS EQUAL TO RAMDOM NUMBER R2
S458
GENERATE RAMDOM NUMBER Sa
S459
APPLY HASH FUNCTION BASED ON KEY Kla TO RAMDOM NUMBER Na, Nb TO FIND RAMDOM NUMBER R3
S460
SEND RAMDOM NUMBER R3 AND RAMDOM NUMBER Sa
S461
RECEIVE RAMDOM NUMBER R3 AND RAMDOM NUMBER Sa
S491
APPLY HASH FUNCTION BASED ON KEY Kab TO RAMDOM NUMBER Nb AND RAMDOM NUMBER Na TO FIND RAMDOM NUMBER R4
S492
CHECK IF RAMDOM NUMBER R3 IS EQUAL TO RAMDOM NUMBER R4
S493
APPLY HASH FUNCTION BASED ON KEY K'ab TO RAMDOM NUMBER Sa AND Sb TO FIND TRANSIENT KEY Ks
S462
APPLY HASH FUNCTION BASED ON KEY K'ab TO RAMDOM NUMBER Sa AND Sb TO FIND TRANSIENT KEY Ks
S494

FIG.41

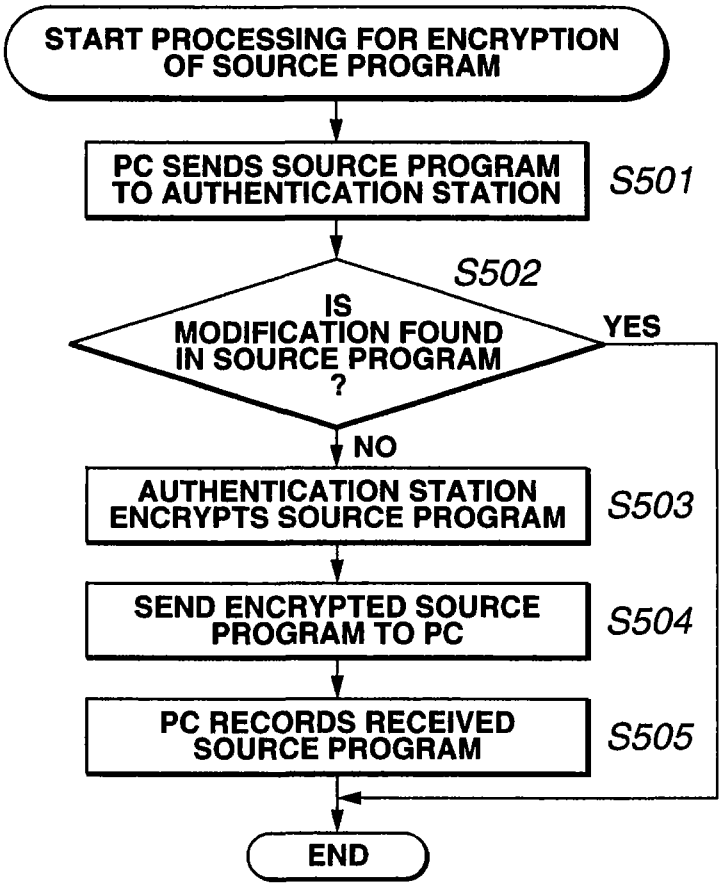

START PROCESSING FOR ENCRYPTION OF SOURCE PROGRAM
PC SENDS SOURCE PROGRAM TO AUTHENTICATION STATION
S501
S502
IS MODIFICATION FOUND IN SOURCE PROGRAM ?
YES
NO
AUTHENTICATION STATION ENCRYPTS SOURCE PROGRAM
S503
SEND ENCRYPTED SOURCE PROGRAM TO PC
S504
PC RECORDS RECEIVED SOURCE PROGRAM
S505
END

FIG.42

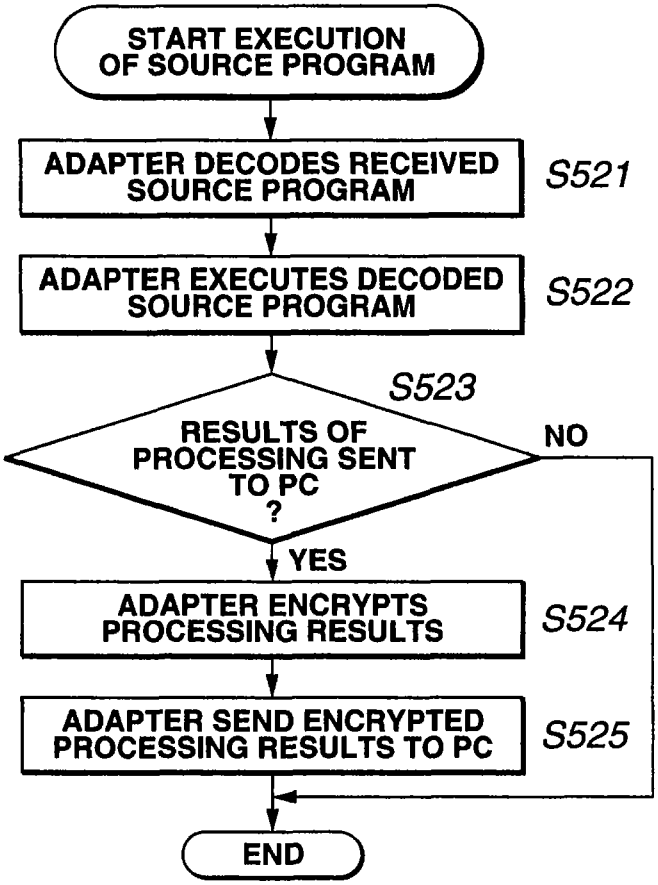

START EXECUTION OF SOURCE PROGRAM
ADAPTER DECODES RECEIVED SOURCE PROGRAM
S521
ADAPTER EXECUTES DECODED SOURCE PROGRAM
S522
S523
RESULTS OF PROCESSING SENT TO PC ?
NO
YES
ADAPTER ENCRYPTS PROCESSING RESULTS
S524
ADAPTER SEND ENCRYPTED PROCESSING RESULTS TO PC
S525
END

FIG.43

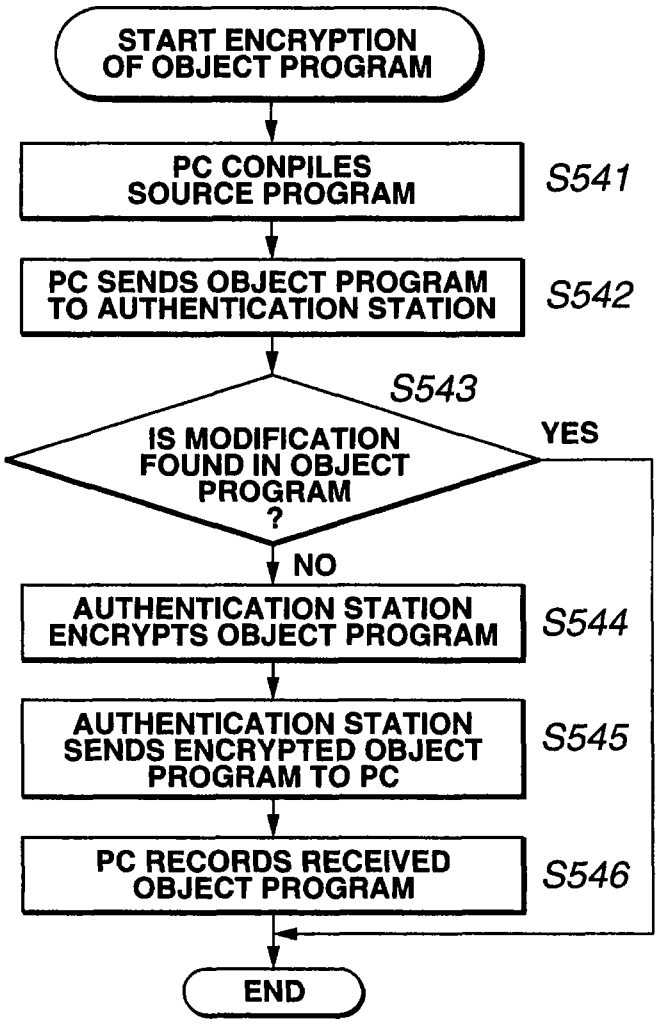

START ENCRYPTION OF OBJECT PROGRAM
PC CONPILES SOURCE PROGRAM
S541
PC SENDS OBJECT PROGRAM TO AUTHENTICATION STATION
S542
S543
IS MODIFICATION FOUND IN OBJECT PROGRAM ?
YES
NO
AUTHENTICATION STATION ENCRYPTS OBJECT PROGRAM
S544
AUTHENTICATION STATION SENDS ENCRYPTED OBJECT PROGRAM TO PC
S545
PC RECORDS RECEIVED OBJECT PROGRAM
S546
END

FIG.44

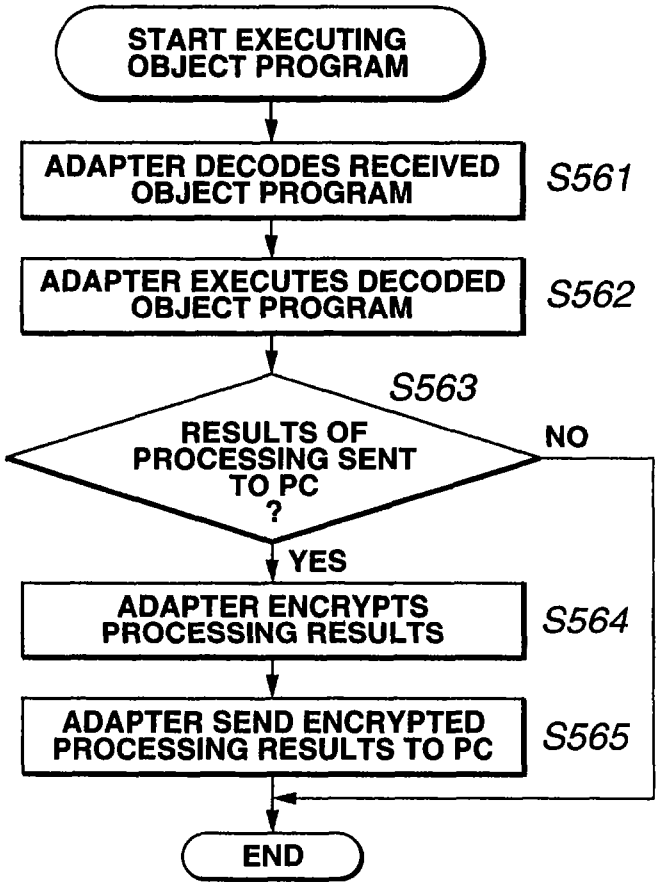

START EXECUTING OBJECT PROGRAM
ADAPTER DECODES RECEIVED OBJECT PROGRAM
S561
ADAPTER EXECUTES DECODED OBJECT PROGRAM
S562
S563
RESULTS OF PROCESSING SENT TO PC ?
NO
YES
ADAPTER ENCRYPTS PROCESSING RESULTS
S564
ADAPTER SEND ENCRYPTED PROCESSING RESULTS TO PC
S565
END

FIG.45

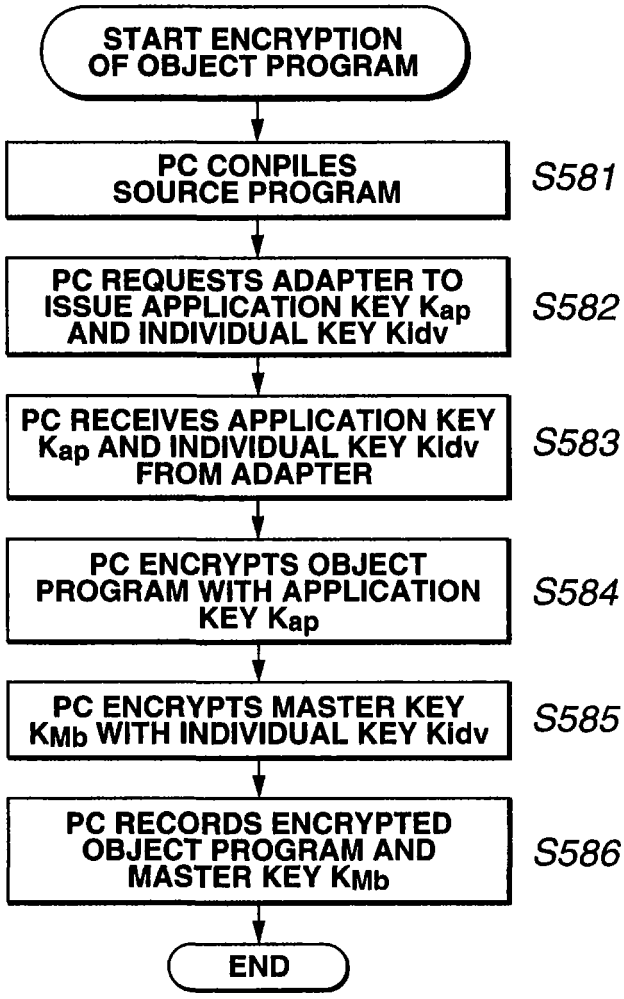

START ENCRYPTION OF OBJECT PROGRAM
PC CONPILES SOURCE PROGRAM
S581
PC REQUESTS ADAPTER TO ISSUE APPLICATION KEY Kap AND INDIVIDUAL KEY Kidv
S582
PC RECEIVES APPLICATION KEY Kap AND INDIVIDUAL KEY Kidv FROM ADAPTER
S583
PC ENCRYPTS OBJECT PROGRAM WITH APPLICATION KEY Kap
S584
PC ENCRYPTS MASTER KEY KMb WITH INDIVIDUAL KEY Kidv
S585
PC RECORDS ENCRYPTED OBJECT PROGRAM AND MASTER KEY KMb
S586
END

FIG.46

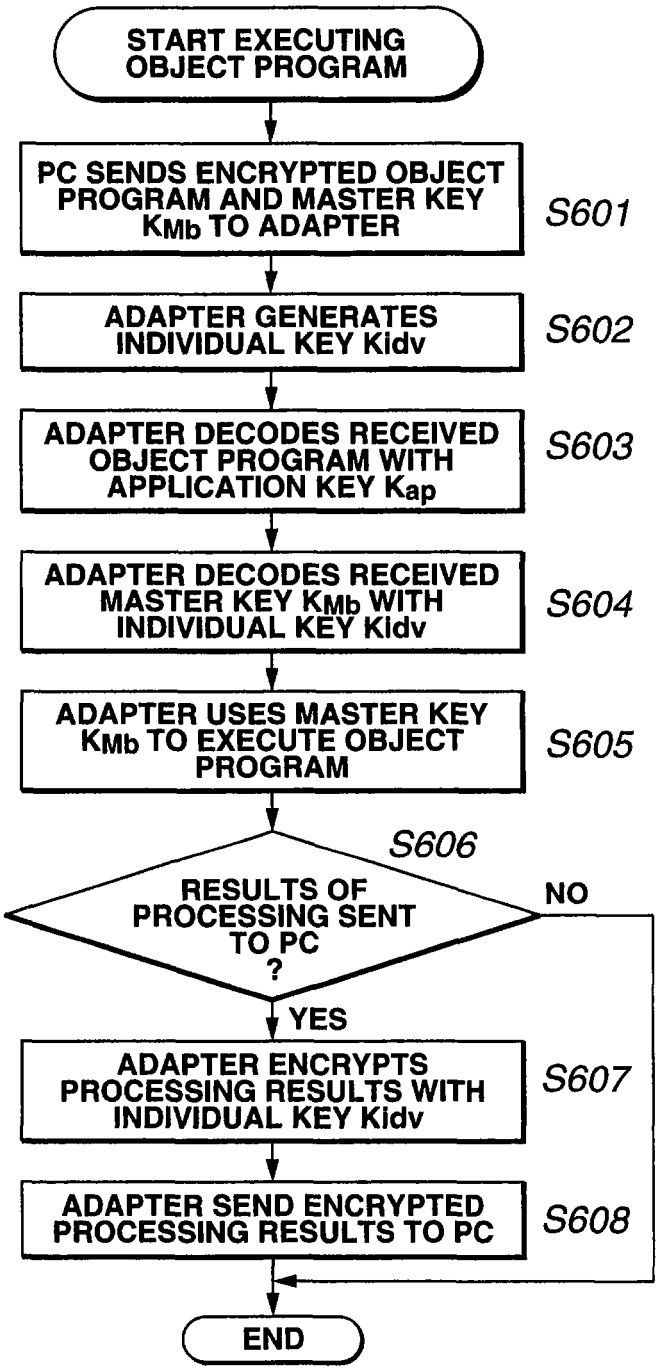

START EXECUTING OBJECT PROGRAM
PC SENDS ENCRYPTED OBJECT PROGRAM AND MASTER KEY KMb TO ADAPTER
S601
ADAPTER GENERATES INDIVIDUAL KEY Kidv
S602
ADAPTER DECODES RECEIVED OBJECT PROGRAM WITH APPLICATION KEY Kap
S603
ADAPTER DECODES RECEIVED MASTER KEY KMb WITH INDIVIDUAL KEY Kidv
S604
ADAPTER USES MASTER KEY KMb TO EXECUTE OBJECT PROGRAM
S605
S606
RESULTS OF PROCESSING SENT TO PC ?
NO
YES
ADAPTER ENCRYPTS PROCESSING RESULTS WITH INDIVIDUAL KEY Kidv
S607
ADAPTER SEND ENCRYPTED PROCESSING RESULTS TO PC
S608
END

FIG.47

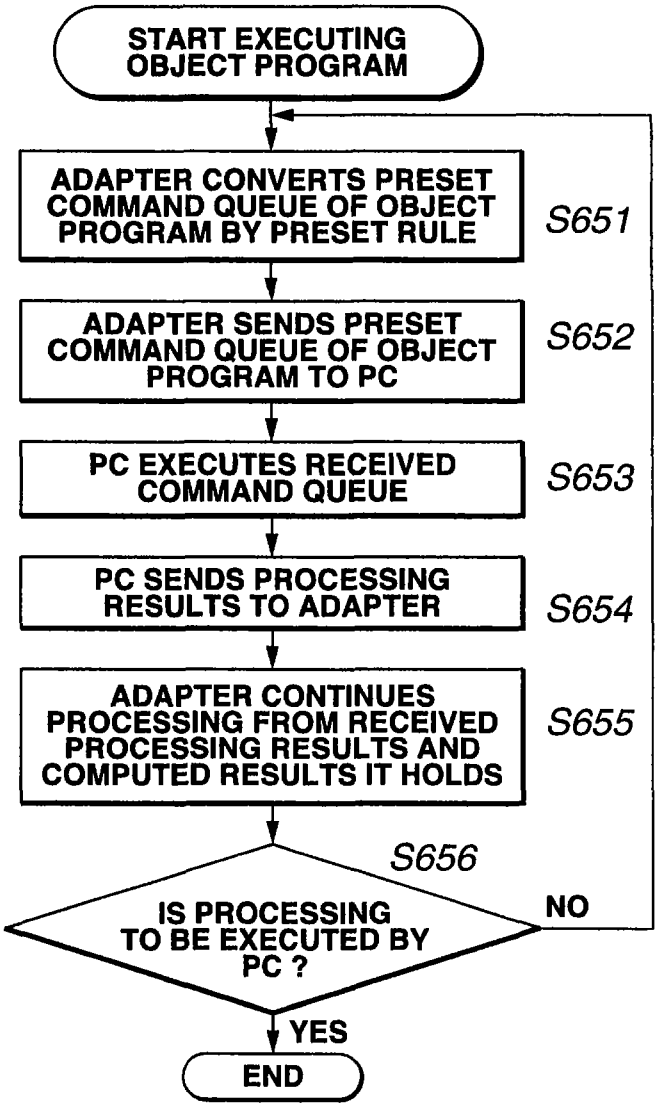

START EXECUTING OBJECT PROGRAM
ADAPTER CONVERTS PRESET COMMAND QUEUE OF OBJECT PROGRAM BY PRESET RULE
S651
ADAPTER SENDS PRESET COMMAND QUEUE OF OBJECT PROGRAM TO PC
S652
PC EXECUTES RECEIVED COMMAND QUEUE
S653
PC SENDS PROCESSING RESULTS TO ADAPTER
S654
ADAPTER CONTINUES PROCESSING FROM RECEIVED PROCESSING RESULTS AND COMPUTED RESULTS IT HOLDS
S655
S656
IS PROCESSING TO BE EXECUTED BY PC ?
NO
YES
END

FIG.48

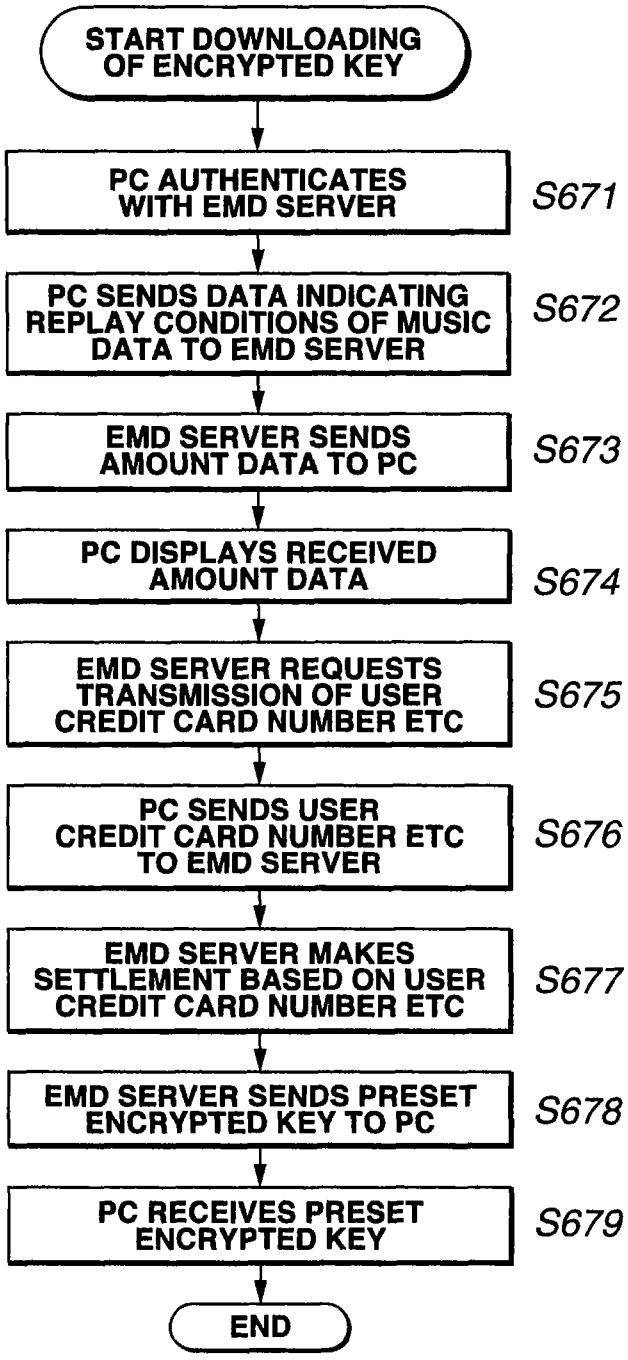

START DOWNLOADING OF ENCRYPTED KEY
PC AUTHENTICATES WITH EMD SERVER
S671
PC SENDS DATA INDICATING REPLAY CONDITIONS OF MUSIC DATA TO EMD SERVER
S672
EMD SERVER SENDS AMOUNT DATA TO PC
S673
PC DISPLAYS RECEIVED AMOUNT DATA
S674
EMD SERVER REQUESTS TRANSMISSION OF USER CREDIT CARD NUMBER ETC
S675
PC SENDS USER CREDIT CARD NUMBER ETC TO EMD SERVER
S676
EMD SERVER MAKES SETTLEMENT BASED ON USER CREDIT CARD NUMBER ETC
S677
EMD SERVER SENDS PRESET ENCRYPTED KEY TO PC
S678
PC RECEIVES PRESET ENCRYPTED KEY
S679
END

FIG.49