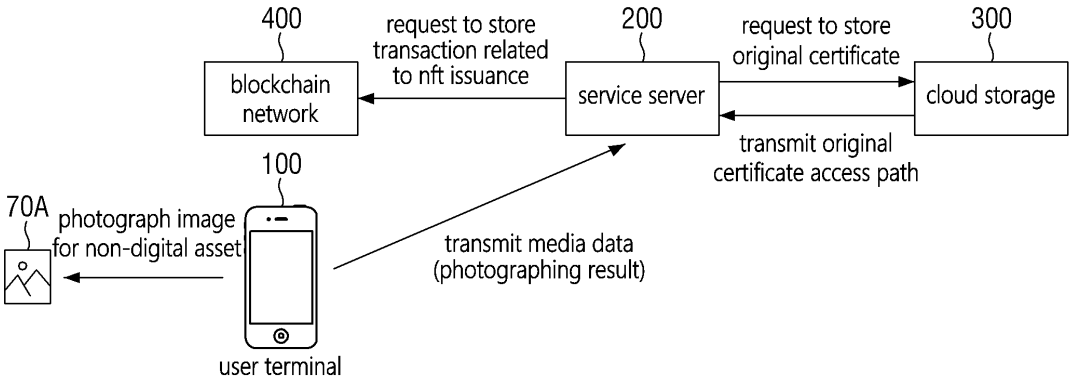

400
blockchain network
request to store transaction related to nft issuance
200
service server
request to store original certificate
300
cloud storage
transmit original certificate access path
100
70A
photograph image for non-digital asset
transmit media data (photographing result)
user terminal

FIG. 1

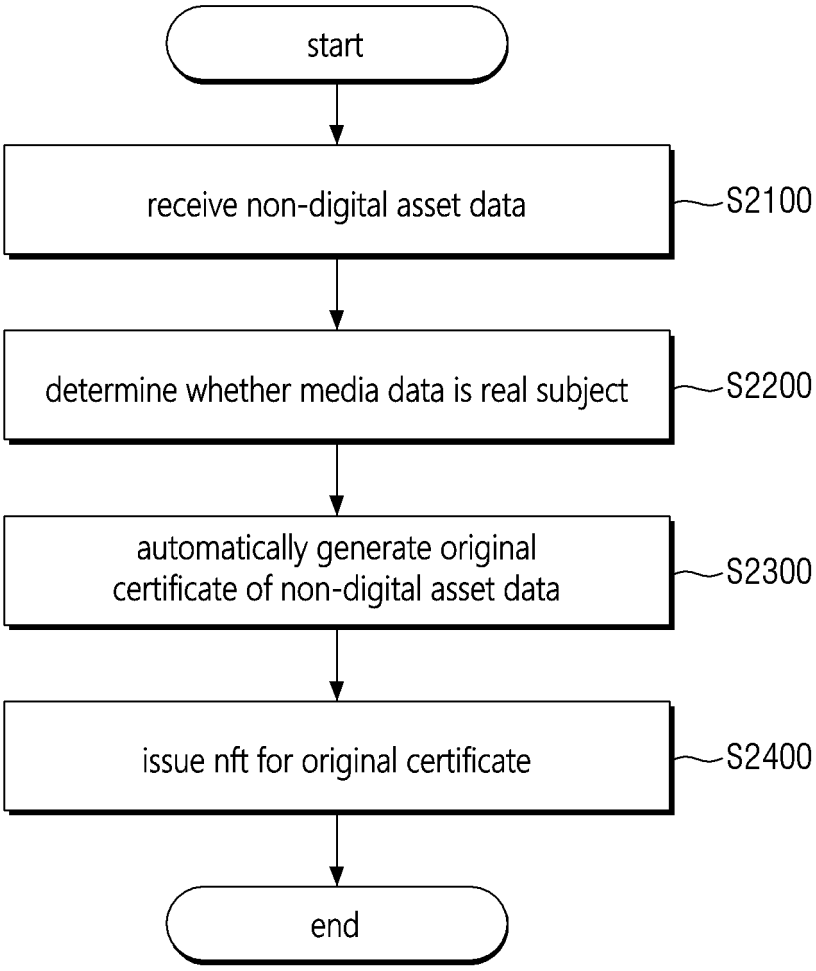

start
receive non-digital asset data
S2100
determine whether media data is real subject
S2200
automatically generate original certificate of non-digital asset data
S2300
issue nft for original certificate
S2400
end

FIG. 2

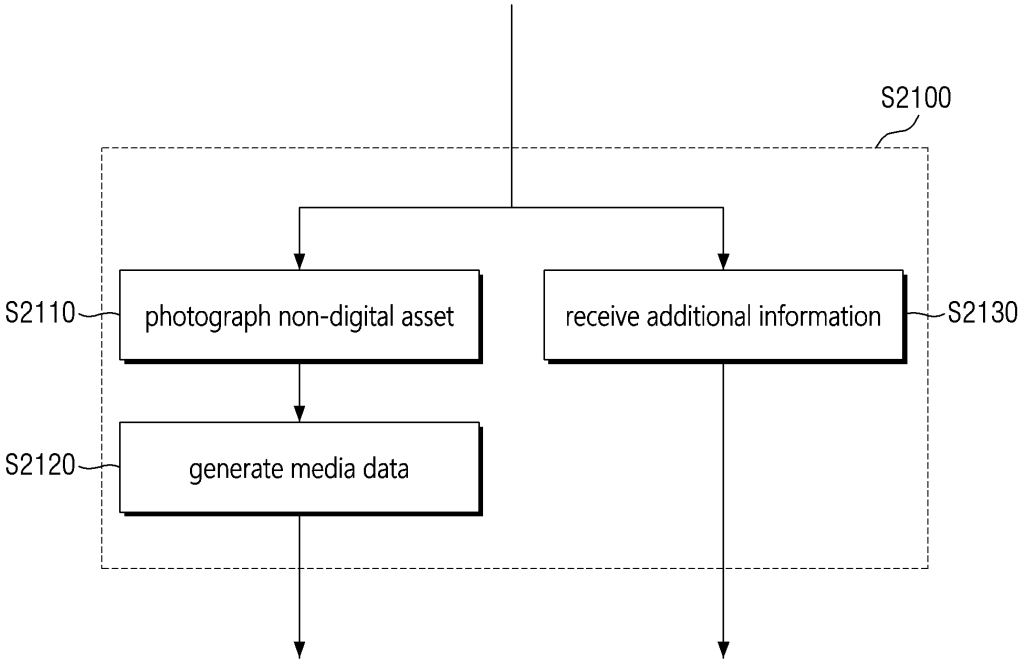

S2100
S2110
photograph non-digital asset
receive additional information
S2130
S2120
generate media data

FIG. 3

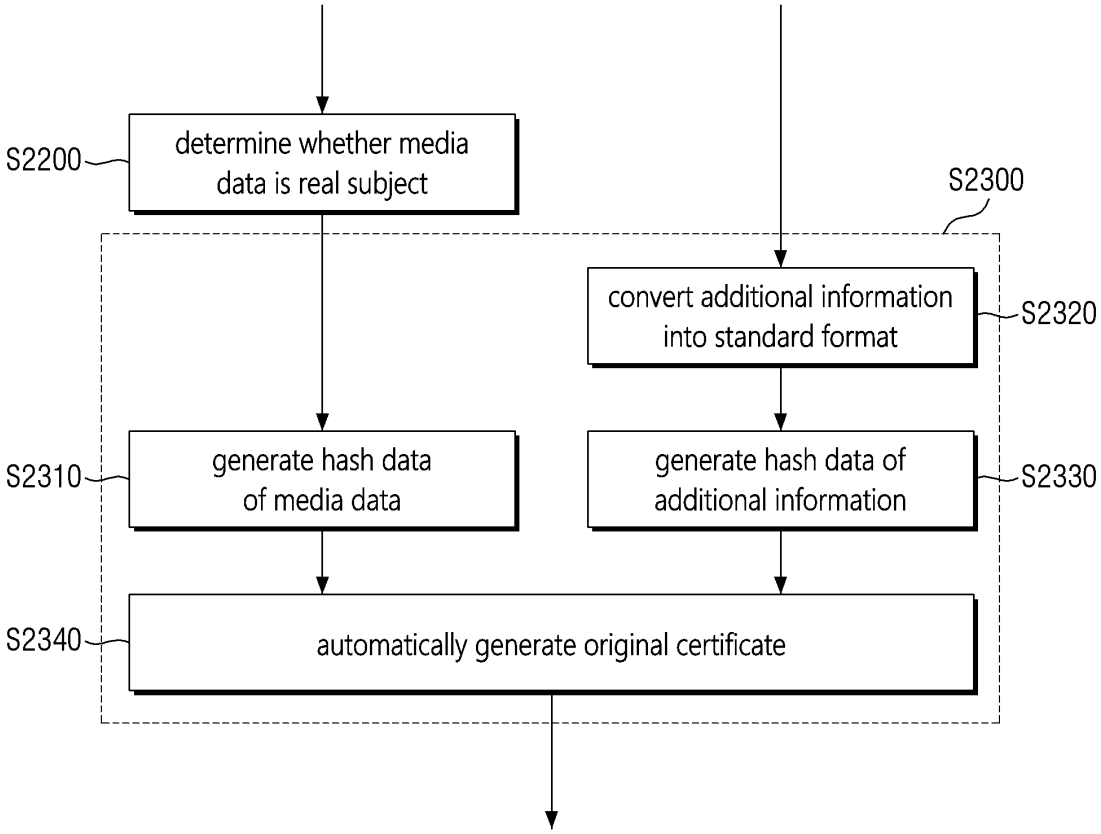

S2200
determine whether media data is real subject
S2300
convert additional information into standard format
S2320
S2310
generate hash data of media data
generate hash data of additional information
S2330
S2340
automatically generate original certificate

FIG. 4

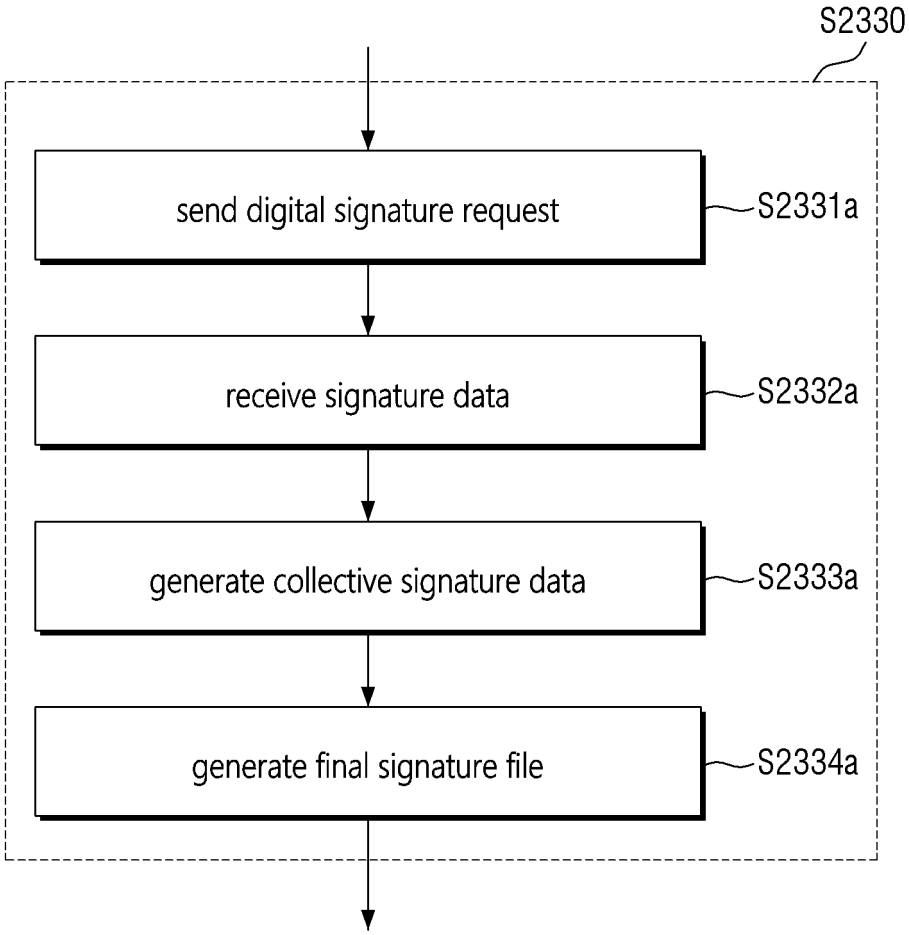

S2330
send digital signature request
S2331a
receive signature data
S2332a
generate collective signature data
S2333a
generate final signature file
S2334a

FIG. 5

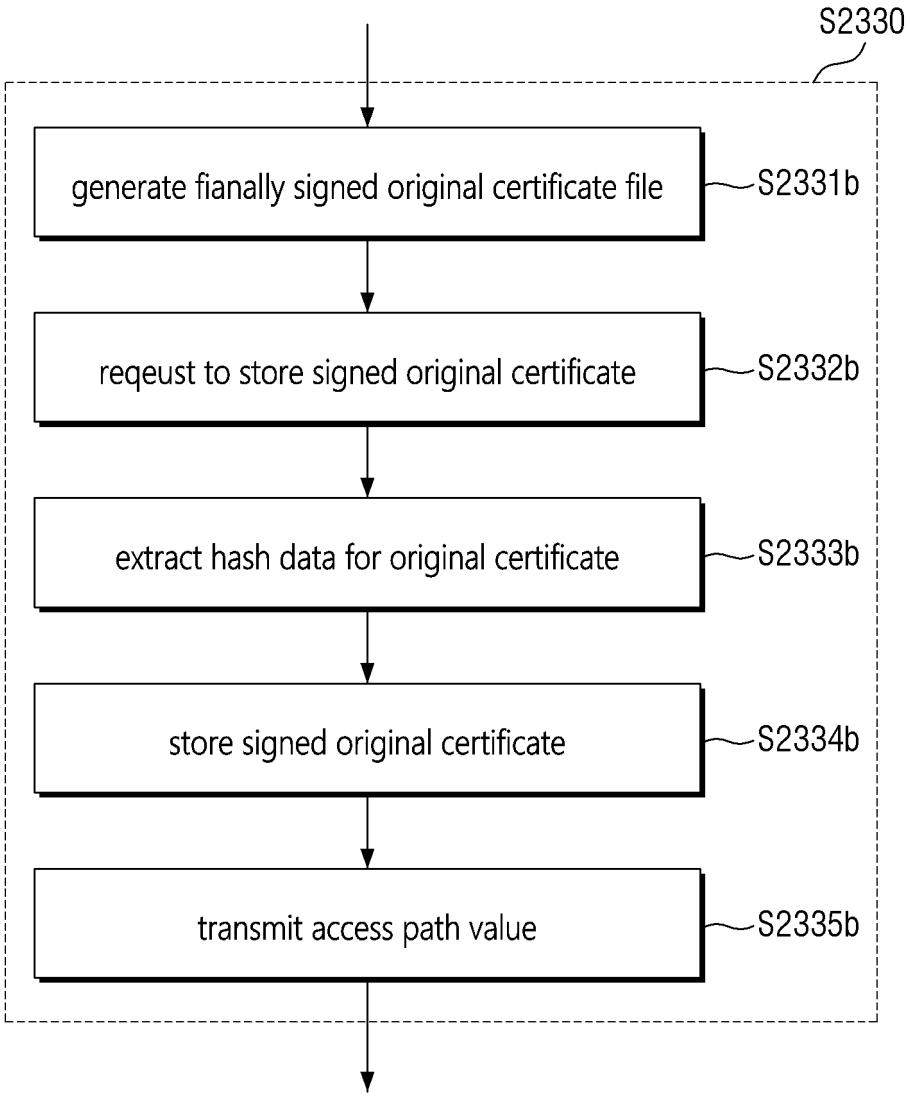

S2330
generate fianally signed original certificate file
S2331b
reqeust to store signed original certificate
S2332b
extract hash data for original certificate
S2333b
store signed original certificate
S2334b
transmit access path value
S2335b

FIG. 6

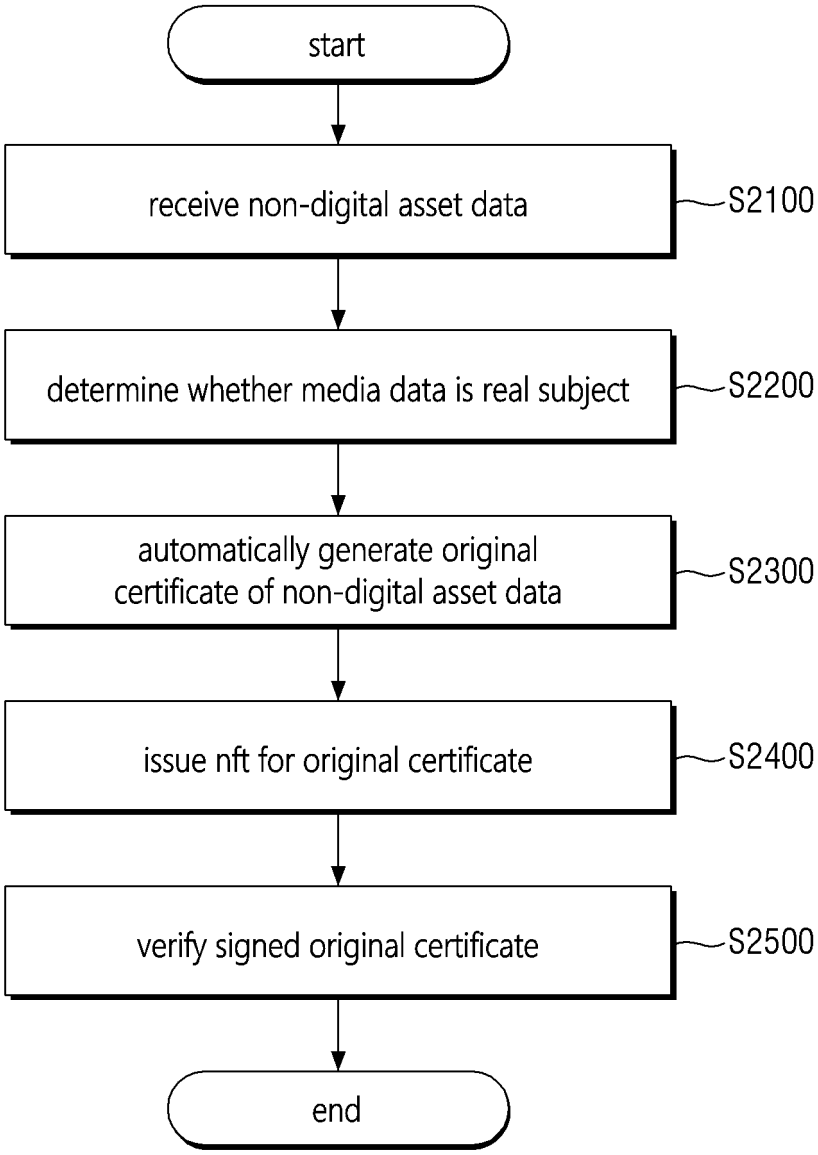

start
receive non-digital asset data
S2100
determine whether media data is real subject
S2200
automatically generate original certificate of non-digital asset data
S2300
issue nft for original certificate
S2400
verify signed original certificate
S2500
end

FIG. 7

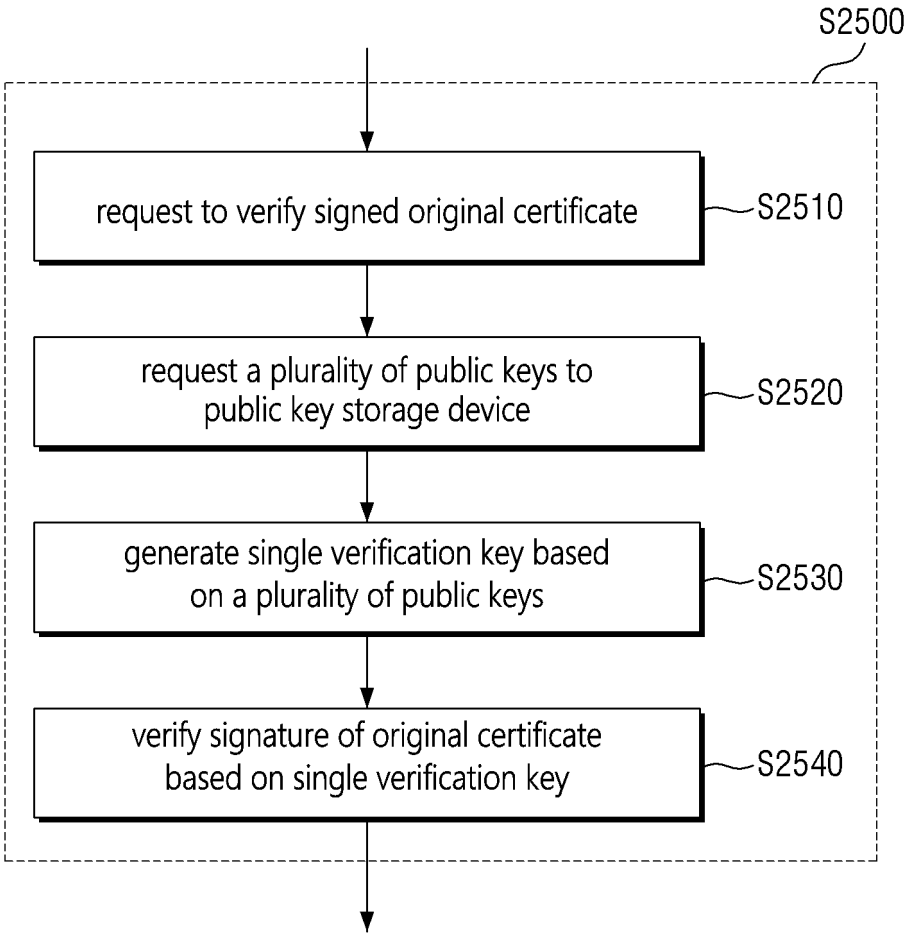

S2500
request to verify signed original certificate
S2510
request a plurality of public keys to public key storage device
S2520
generate single verification key based on a plurality of public keys
S2530
verify signature of original certificate based on single verification key
S2540

FIG. 8

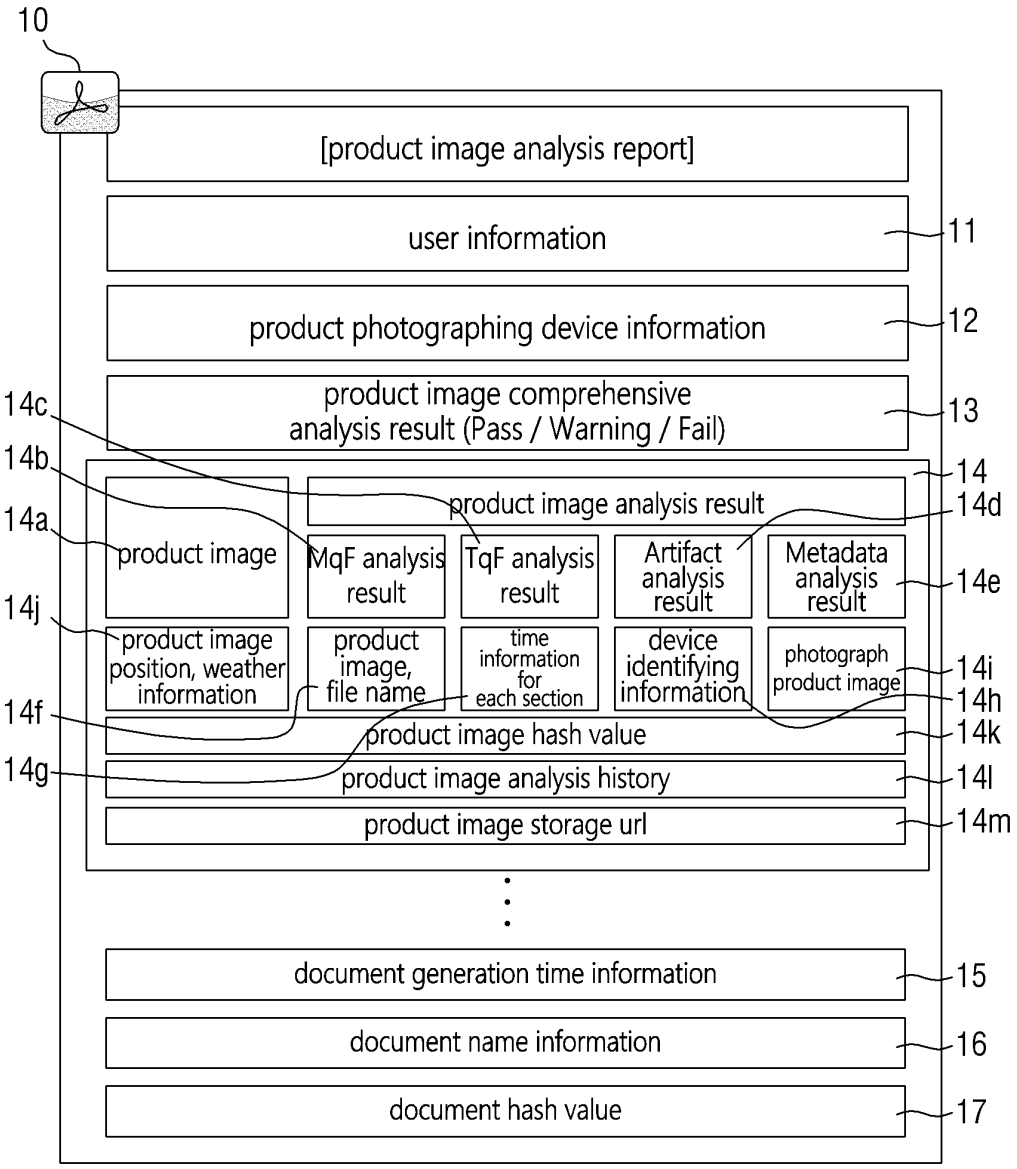

10
[product image analysis report]
user information
11
product photographing device information
12
product image comprehensive analysis result (Pass / Warning / Fail)
13
14c
14b
14a
14j
14f
14g
14
product image analysis result
14d
product image
MqF analysis result
TqF analysis result
Artifact analysis result
Metadata analysis result
14e
product image position, weather information
product image, file name
time information for each section
device identifying information
photograph product image
14i
14h
product image hash value
14k
product image analysis history
14l
product image storage url
14m
document generation time information
15
document name information
16
document hash value
17

FIG. 9

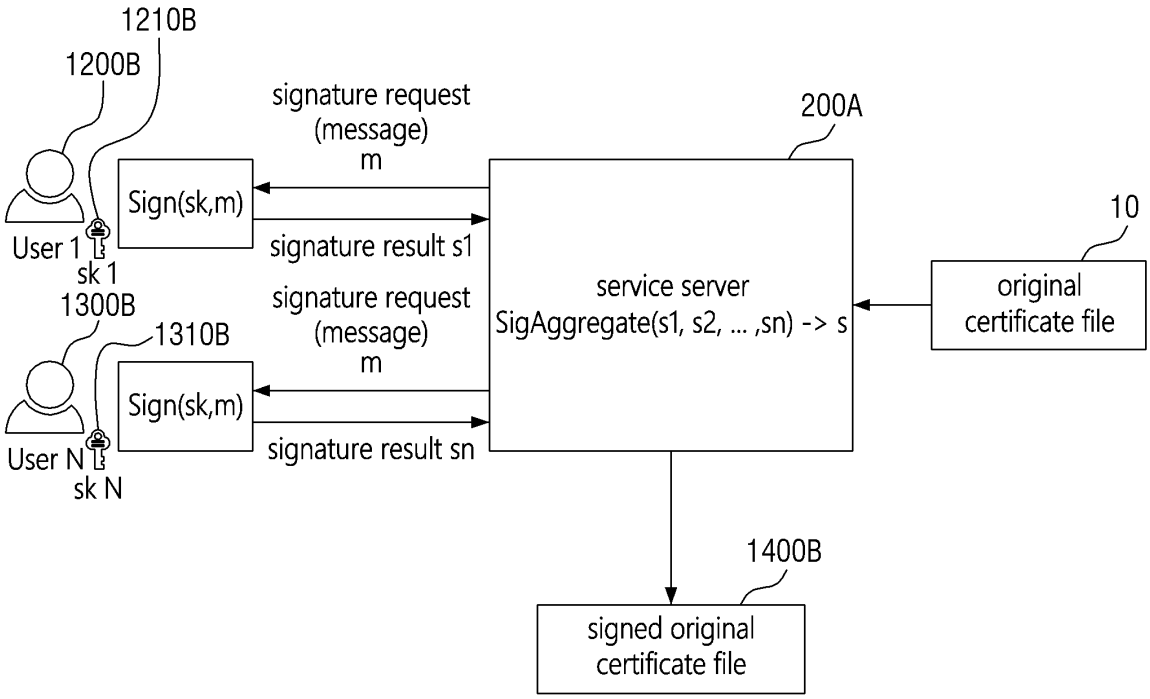

1210B
1200B
signature request
(message)
m
200A
Sign(sk,m)
10
User 1
sk 1
signature result s1
service server
SigAggregate(s1, s2, ... ,sn) -> s
original
certificate file
1300B
1310B
signature request
(message)
m
Sign(sk,m)
User N
sk N
signature result sn
1400B
signed original
certificate file

FIG. 10

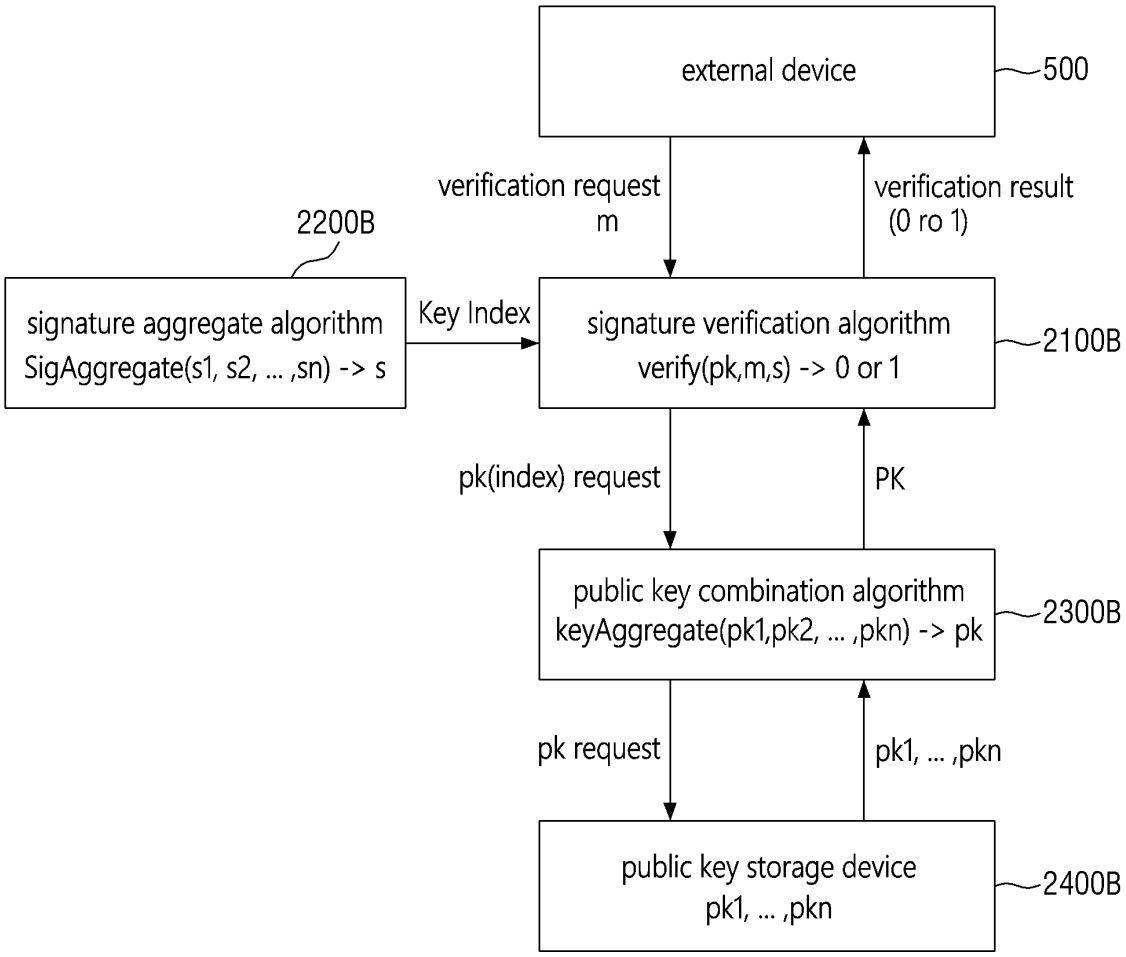

external device
500
verification request
m
verification result
(0 ro 1)
2200B
signature aggregate algorithm
SigAggregate(s1, s2, ... ,sn) -> s
Key Index
signature verification algorithm
verify(pk,m,s) -> 0 or 1
2100B
pk(index) request
PK
public key combination algorithm
keyAggregate(pk1,pk2, ... ,pkn) -> pk
2300B
pk request
pk1, ... ,pkn
public key storage device
pk1, ... ,pkn
2400B

FIG. 11

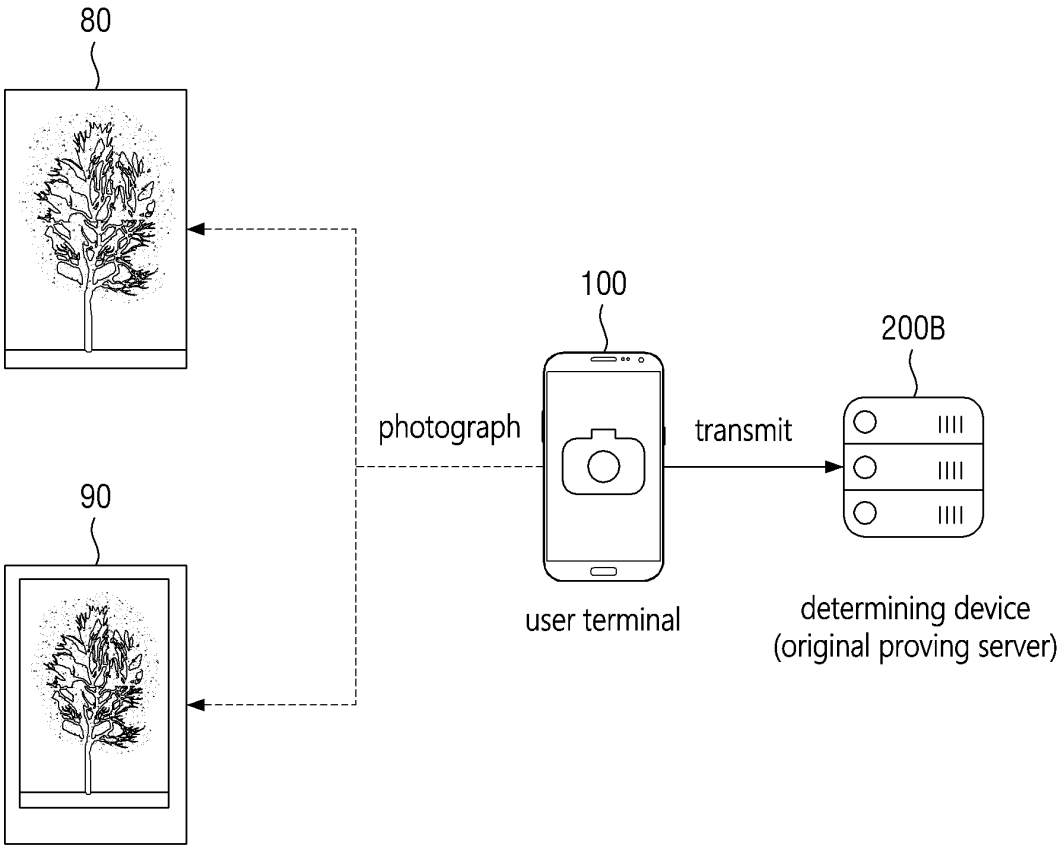

80
90
100
200B
photograph
transmit
user terminal
determining device
(original proving server)

FIG. 12

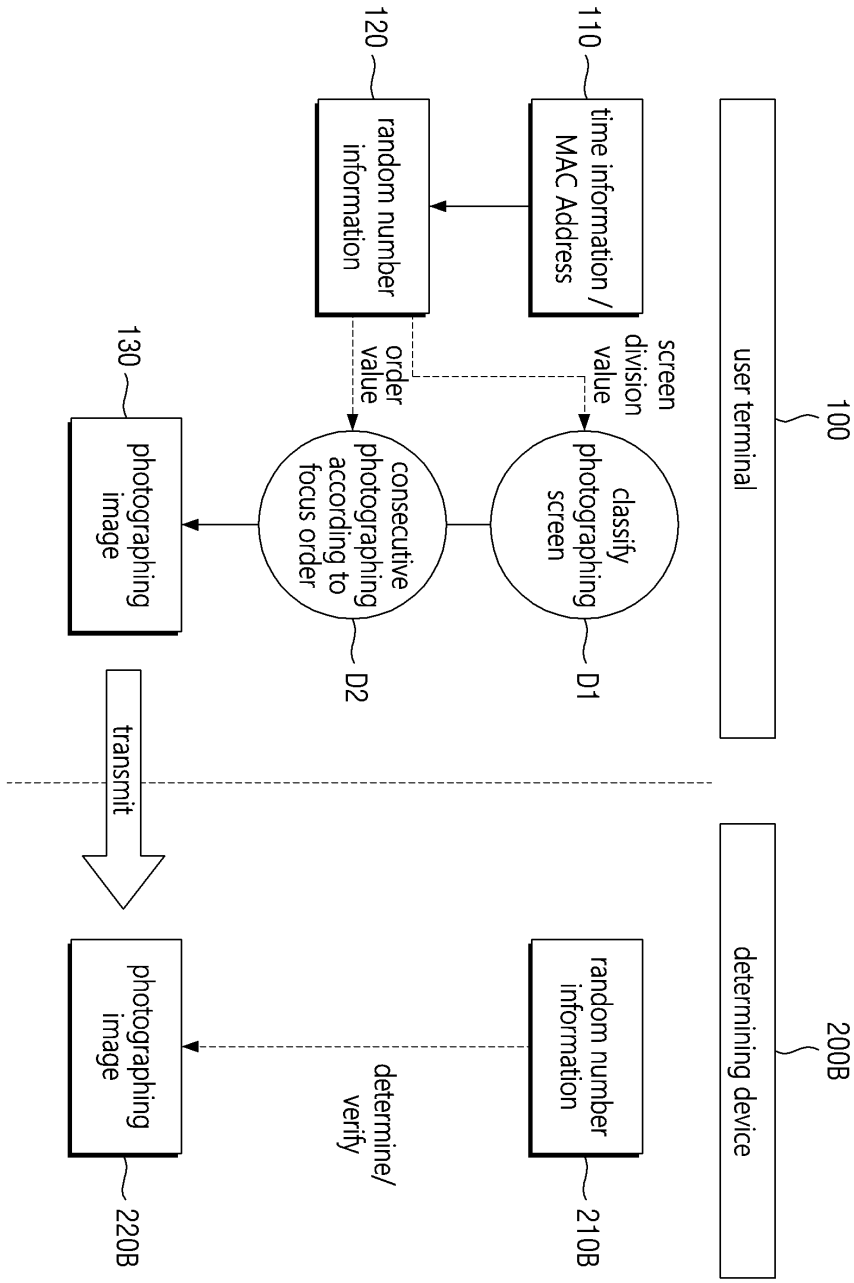

100
user terminal
110
time information / MAC Address
120
random number information
screen division value
order value
130
photographing image
classify photographing screen
consecutive photographing according to focus order
D1
D2
transmit
200B
determining device
210B
random number information
determine/ verify
220B
photographing image

FIG. 13

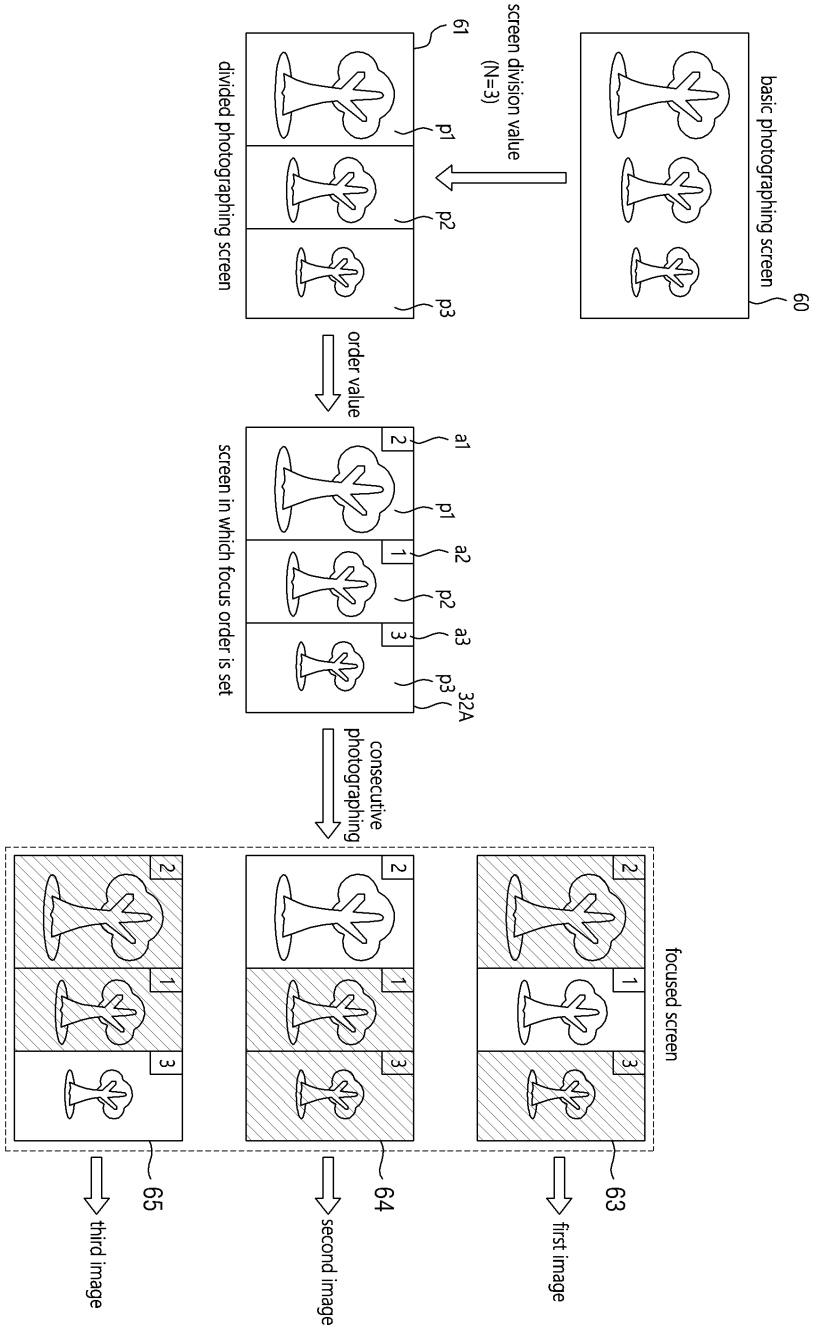

basic photographing screen
60
screen division value
(N=3)
61
p1
p2
p3
divided photographing screen
order value
a1
a2
a3
32A
screen in which focus order is set
consecutive
photographing
focused screen
63
first image
64
second image
65
third image

FIG. 14

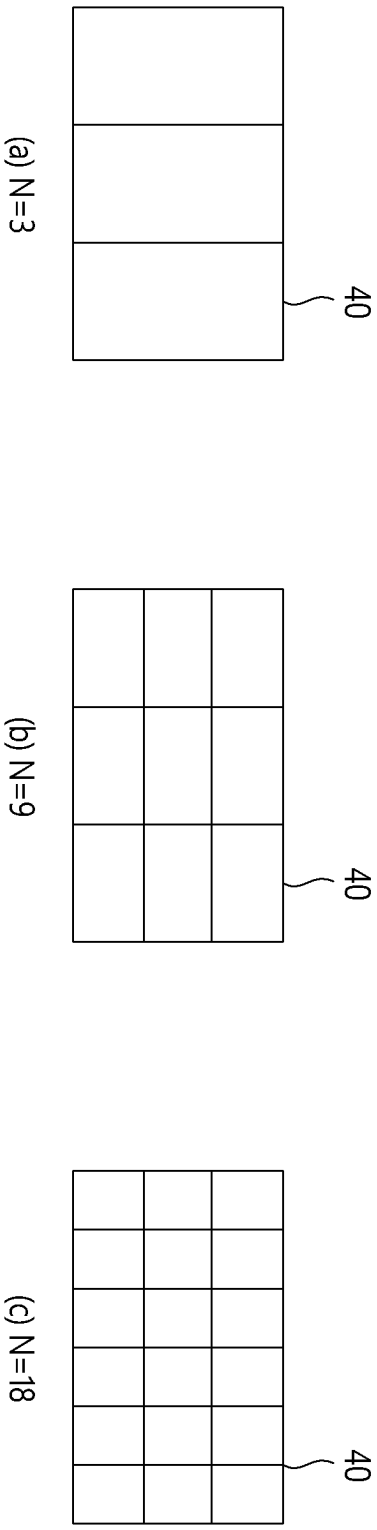


FIG. 15

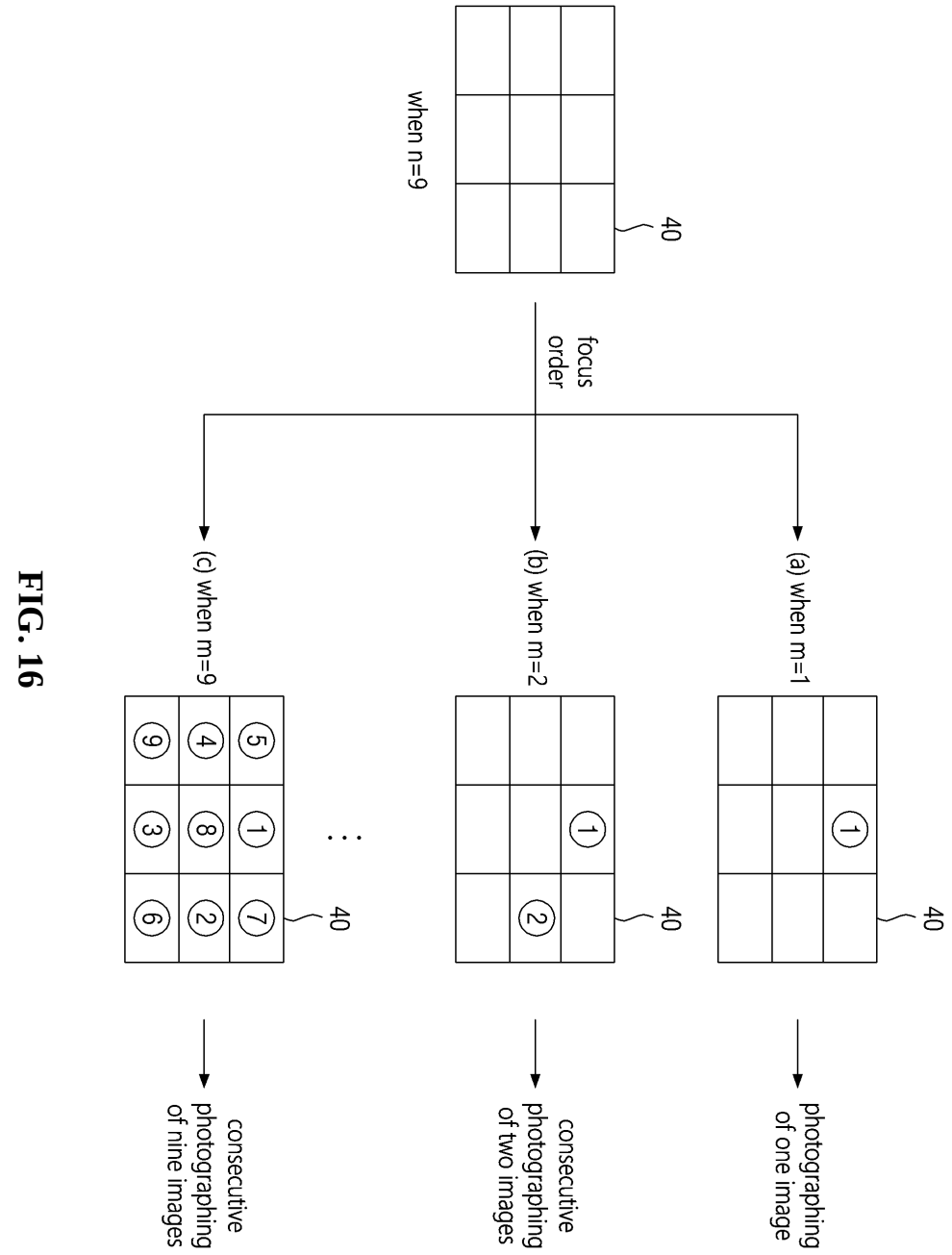

when n=9
40
focus order
(a) when m=1
(b) when m=2
(c) when m=9
1
2
5
1
7
4
8
2
9
3
6
40
40
40
photographing of one image
consecutive photographing of two images
consecutive photographing of nine images

FIG. 16

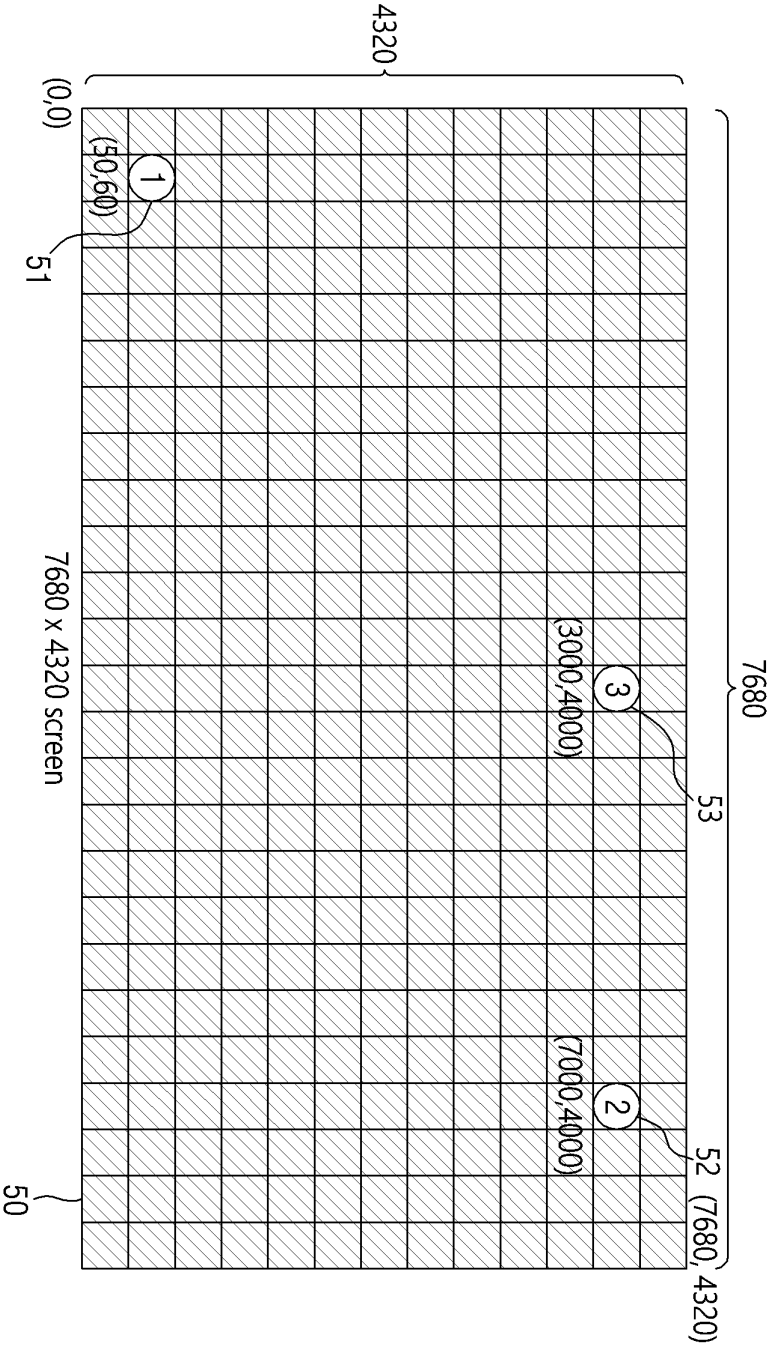

4320
(0,0)
(50,60)
1
51
7680 x 4320 screen
(3000,4000)
3
53
7680
(7000,4000)
2
52
(7680, 4320)
50

FIG. 17

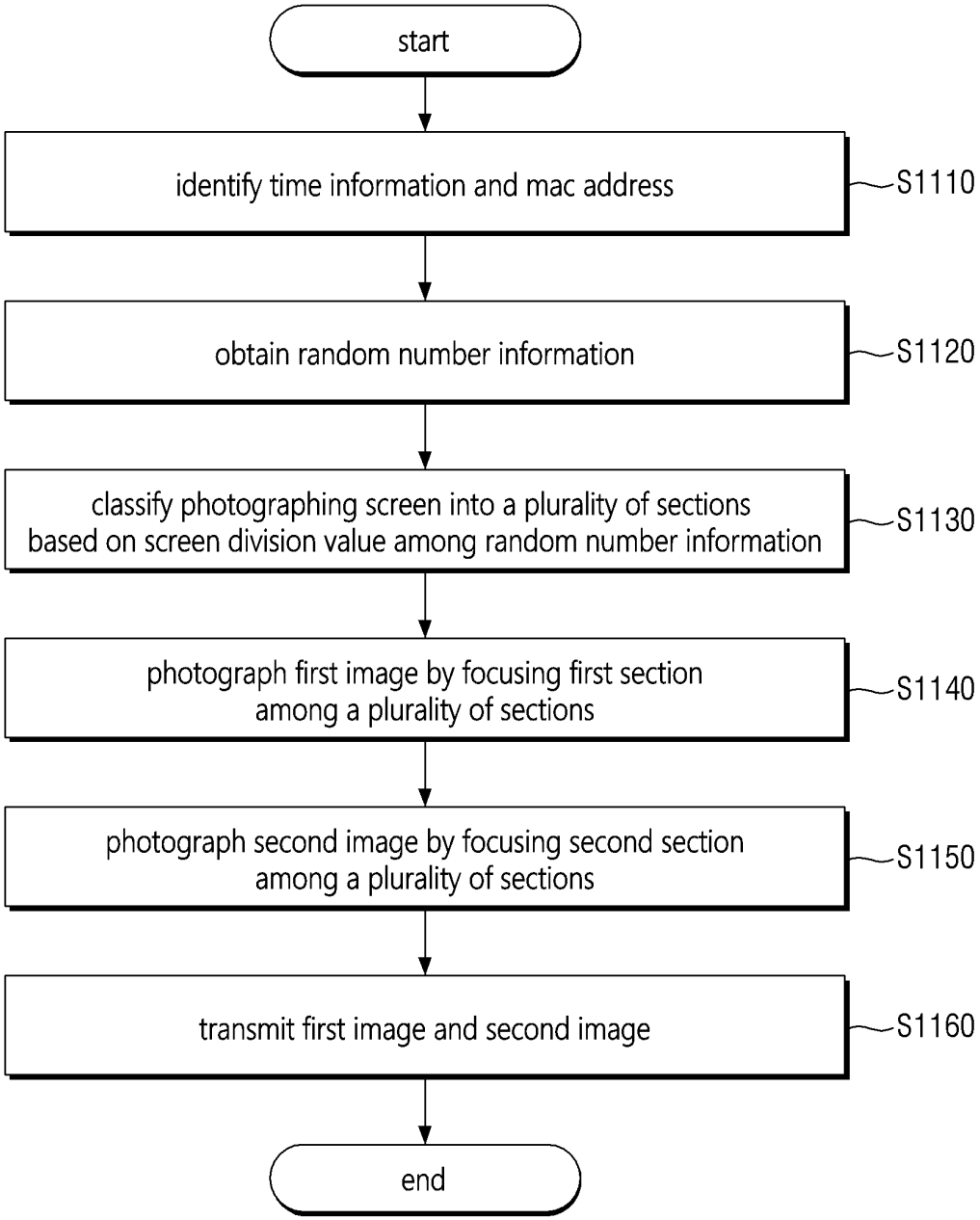

start
identify time information and mac address
S1110
obtain random number information
S1120
classify photographing screen into a plurality of sections based on screen division value among random number information
S1130
photograph first image by focusing first section among a plurality of sections
S1140
photograph second image by focusing second section among a plurality of sections
S1150
transmit first image and second image
S1160
end

FIG. 18

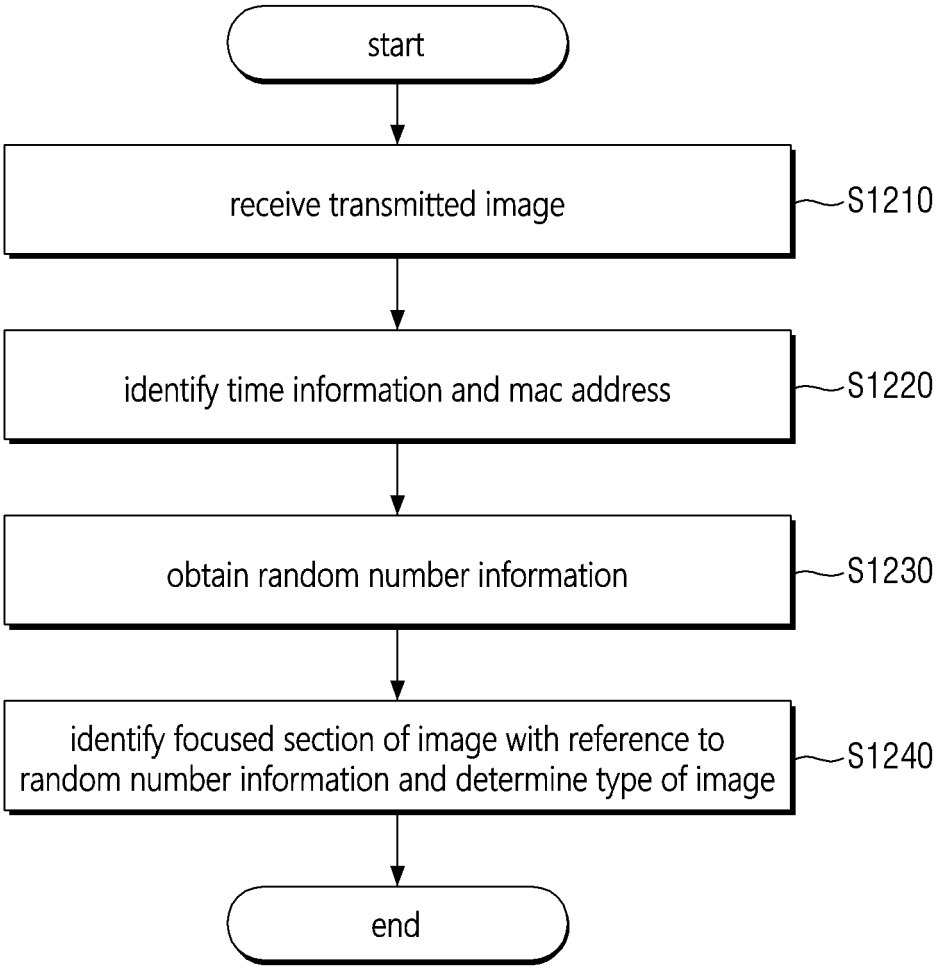

start
receive transmitted image
S1210
identify time information and mac address
S1220
obtain random number information
S1230
identify focused section of image with reference to random number information and determine type of image
S1240
end

FIG. 19

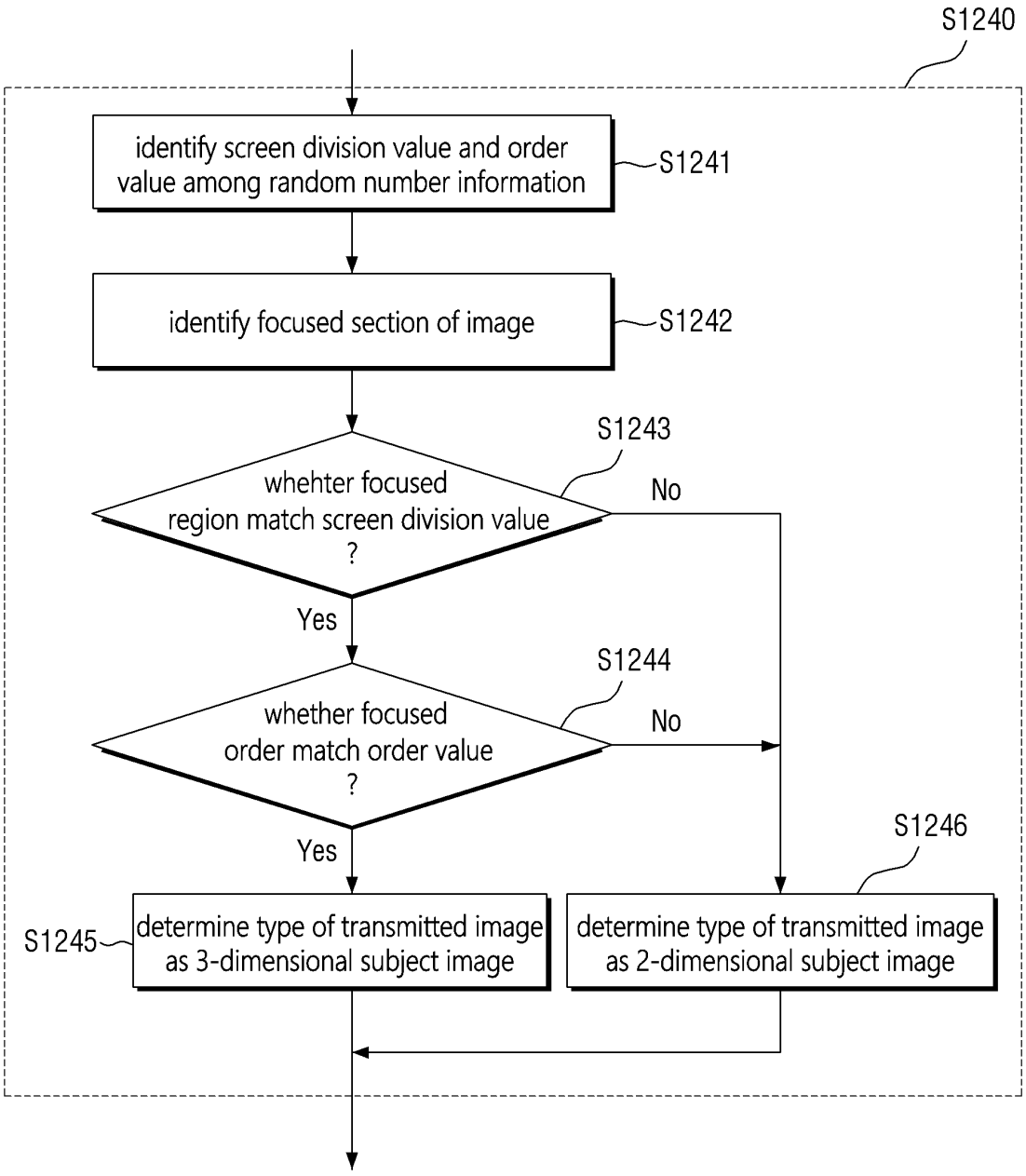

S1240
identify screen division value and order value among random number information
S1241
identify focused section of image
S1242
S1243
whehter focused region match screen division value ?
No
Yes
S1244
whether focused order match order value ?
No
Yes
S1246
S1245
determine type of transmitted image as 3-dimensional subject image
determine type of transmitted image as 2-dimensional subject image

FIG. 20

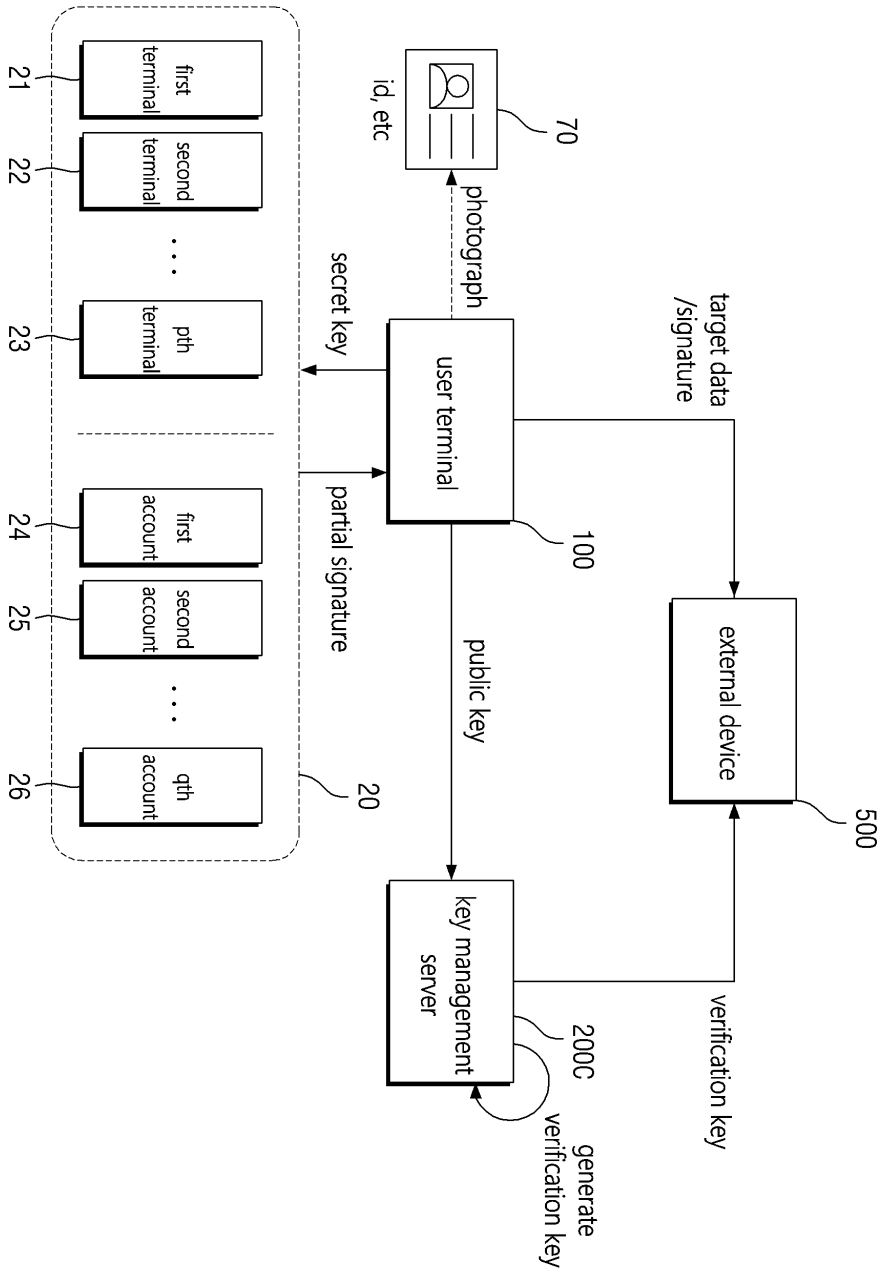

first terminal
second terminal
pth terminal
first account
second account
qth account
21
22
23
24
25
26
20
id, etc
70
photograph
secret key
partial signature
user terminal
100
target data /signature
external device
500
public key
key management server
200C
generate verification key
verification key

FIG. 21

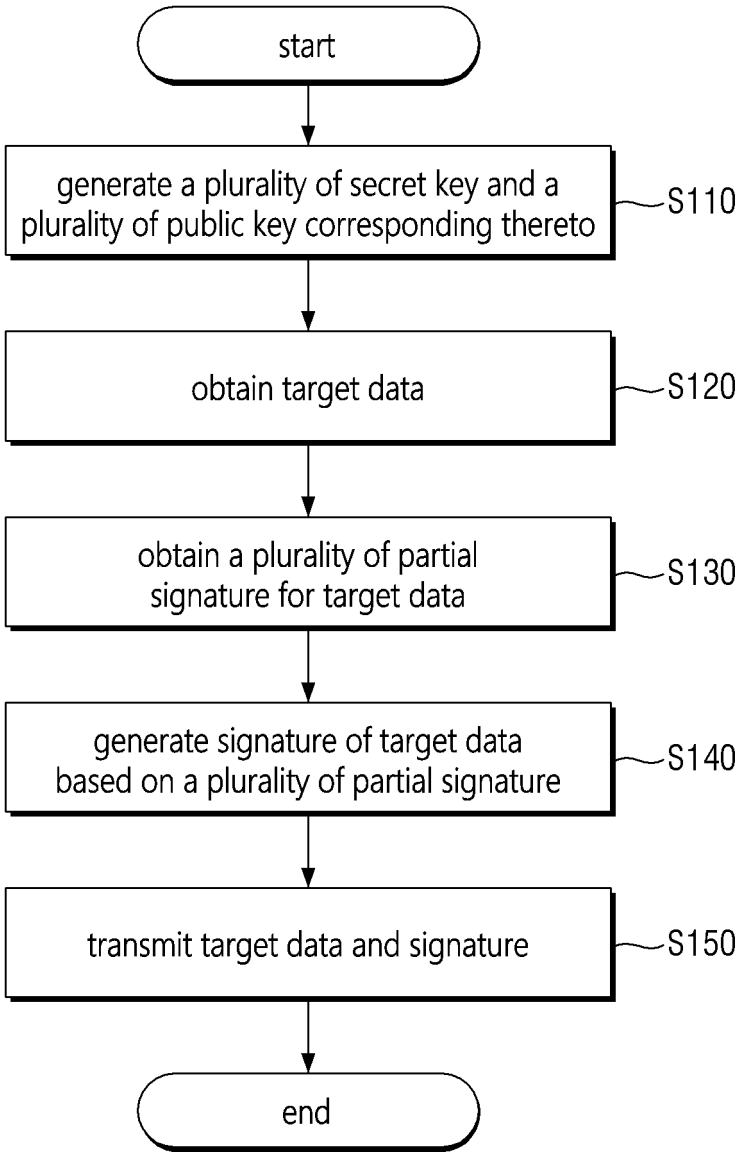

start
generate a plurality of secret key and a plurality of public key corresponding thereto
S110
obtain target data
S120
obtain a plurality of partial signature for target data
S130
generate signature of target data based on a plurality of partial signature
S140
transmit target data and signature
S150
end

FIG. 22

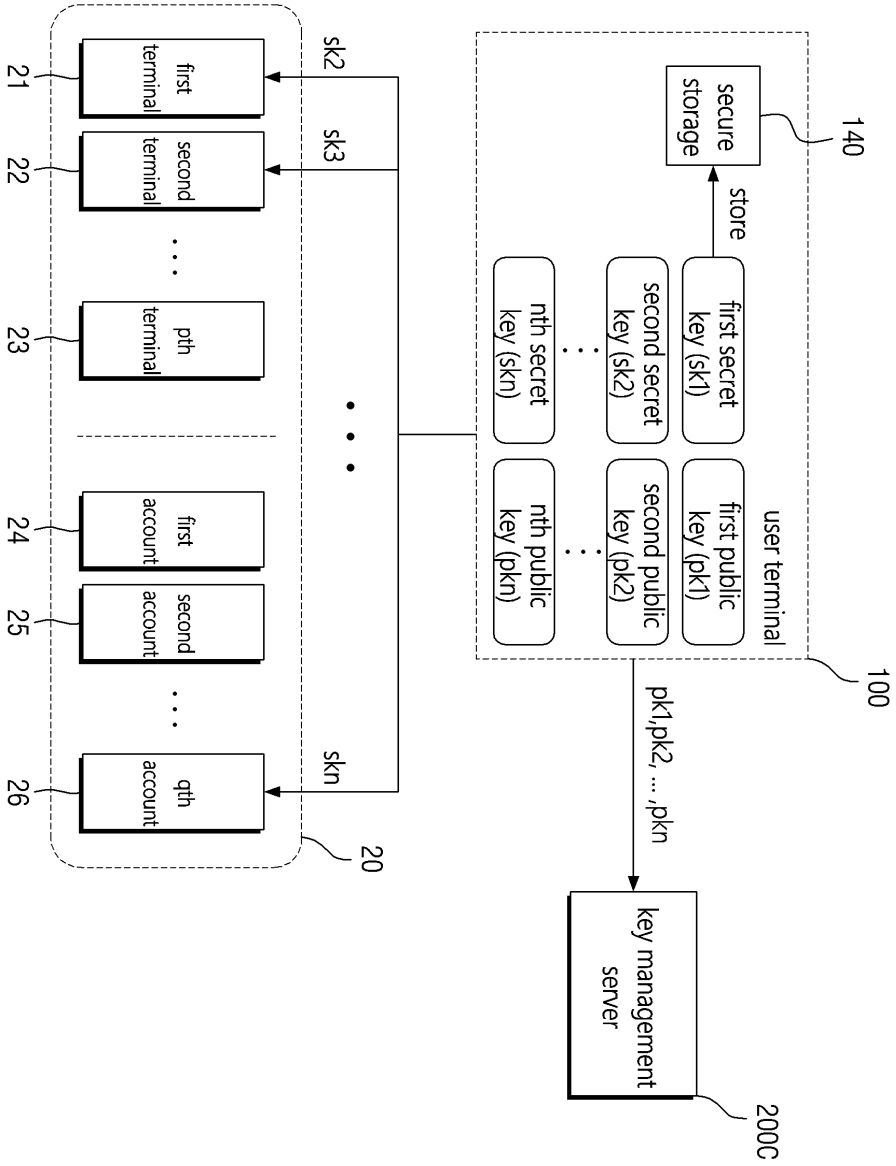

140
secure storage
store
first secret key (sk1)
second secret key (sk2)
nth secret key (skn)
first public key (pk1)
second public key (pk2)
nth public key (pkn)
user terminal
100
pk1,pk2, ... ,pkn
key management server
200C
sk2
sk3
skn
20
21
first terminal
22
second terminal
23
pth terminal
24
first account
25
second account
26
qth account

FIG. 23

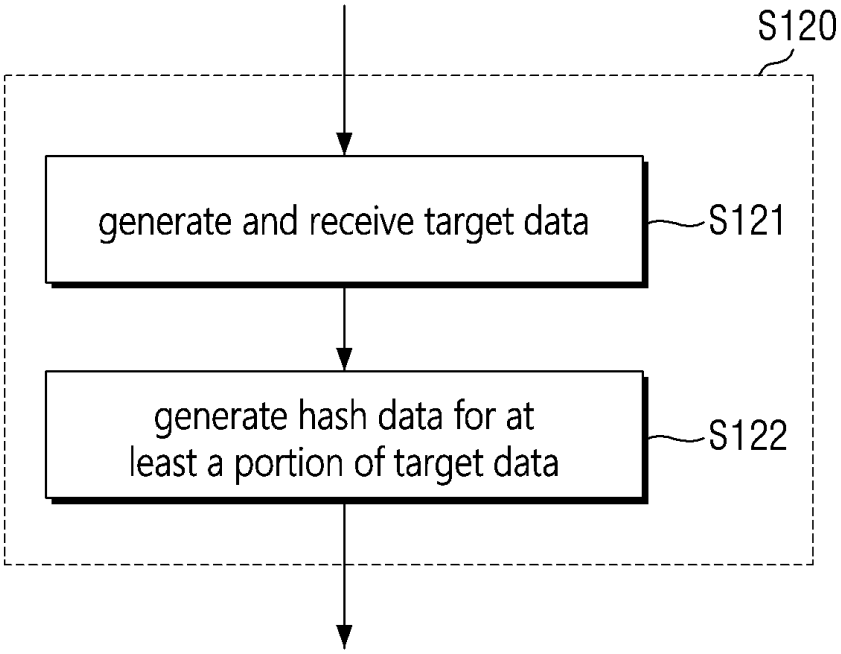

S120
generate and receive target data
S121
generate hash data for at least a portion of target data
S122

FIG. 24

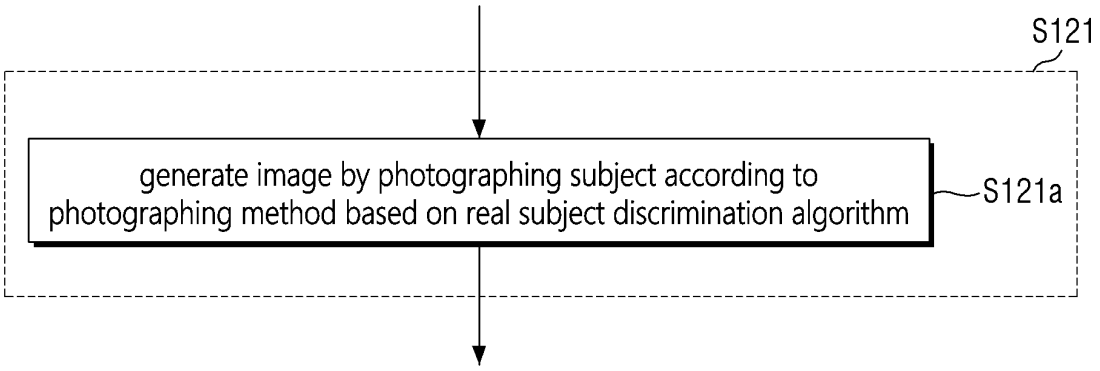

S121
generate image by photographing subject according to photographing method based on real subject discrimination algorithm
S121a

FIG. 25

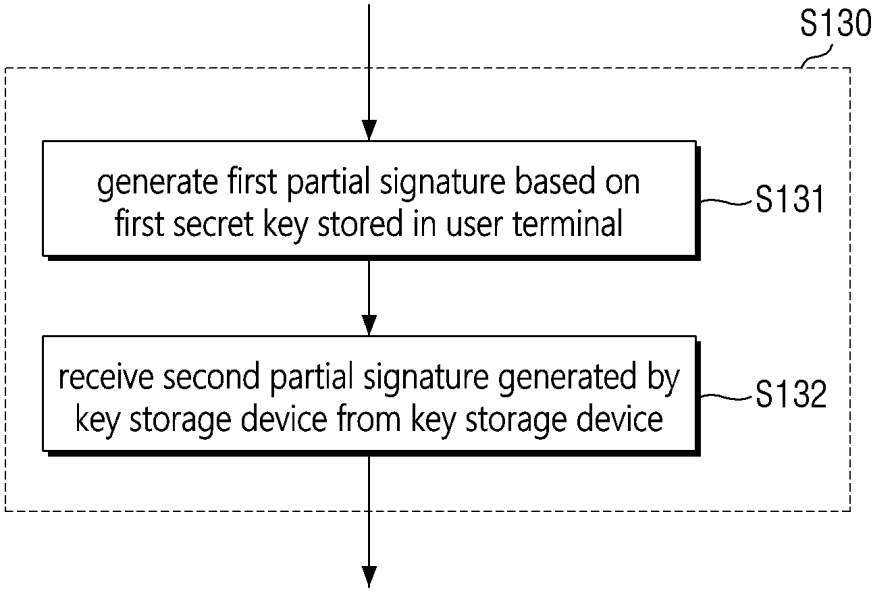

S130
generate first partial signature based on first secret key stored in user terminal
S131
receive second partial signature generated by key storage device from key storage device
S132

FIG. 26

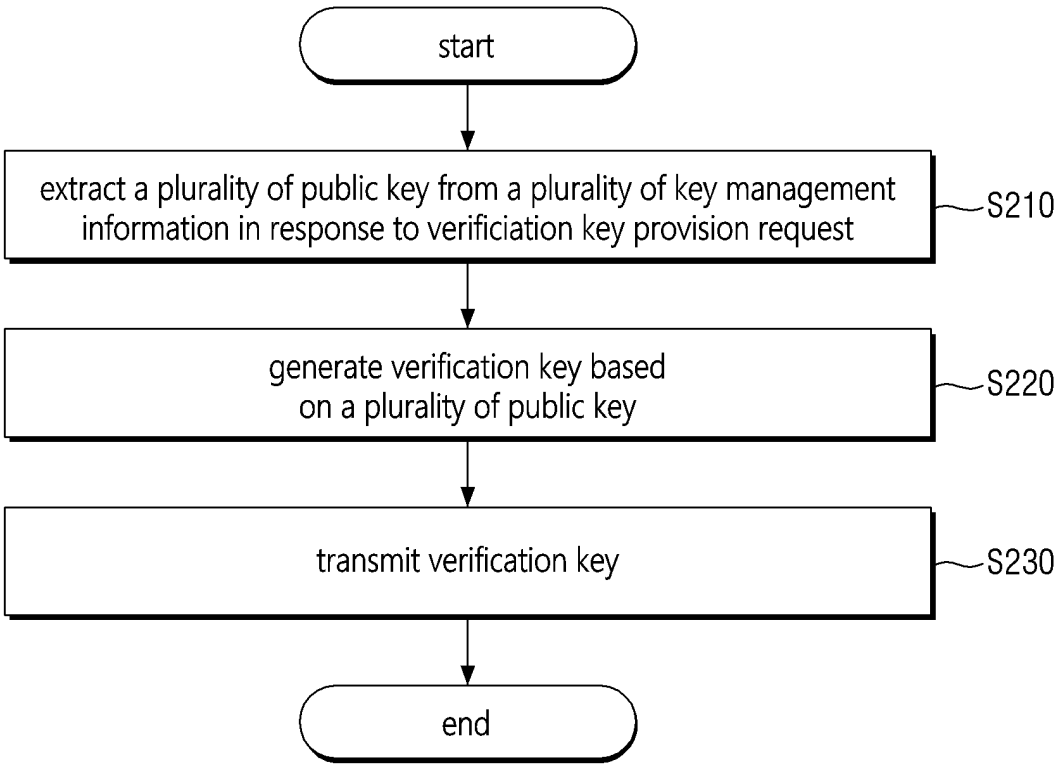

start
extract a plurality of public key from a plurality of key management information in response to verificiation key provision request
S210
generate verification key based on a plurality of public key
S220
transmit verification key
S230
end

FIG. 27

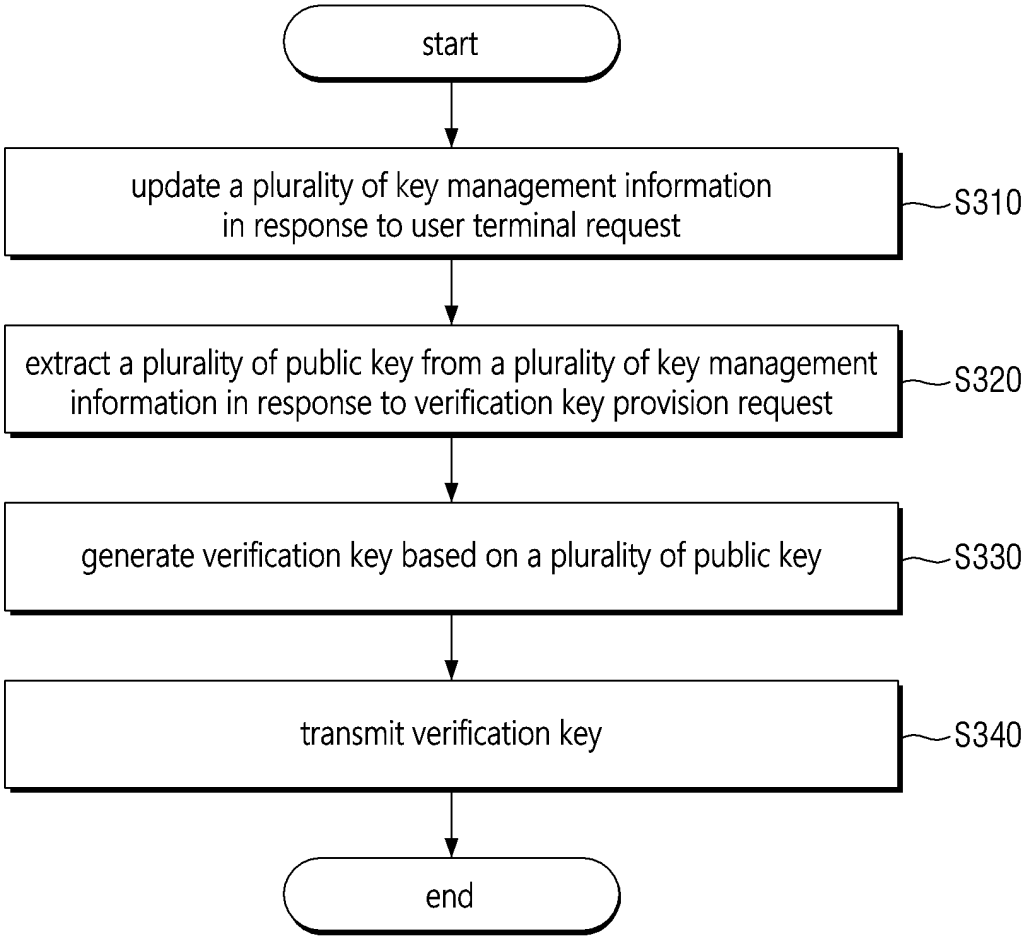

start
update a plurality of key management information in response to user terminal request
S310
extract a plurality of public key from a plurality of key management information in response to verification key provision request
S320
generate verification key based on a plurality of public key
S330
transmit verification key
S340
end

FIG. 28

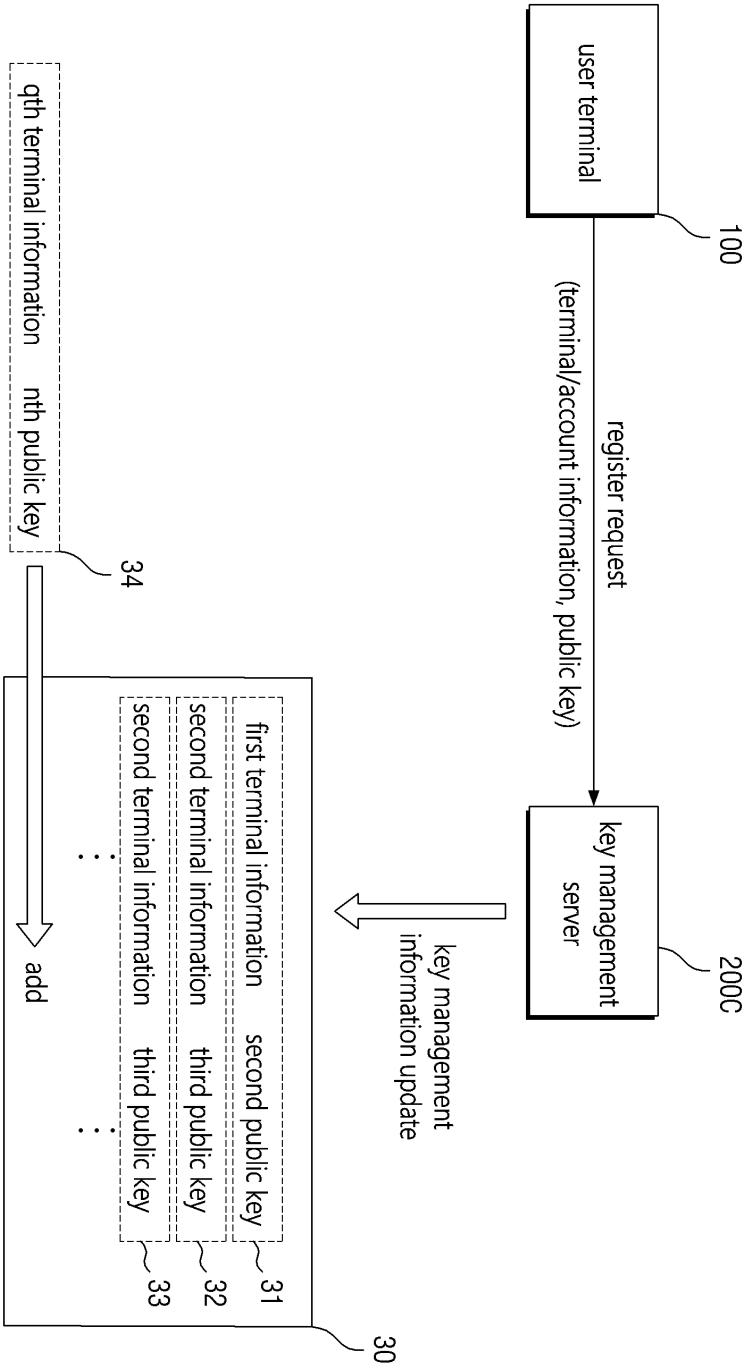

user terminal
100
register request
(terminal/account information, public key)
key management server
200C
key management information update
30
first terminal information second public key
31
second terminal information third public key
32
second terminal information third public key
33
qth terminal information nth public key
34
add

FIG. 29

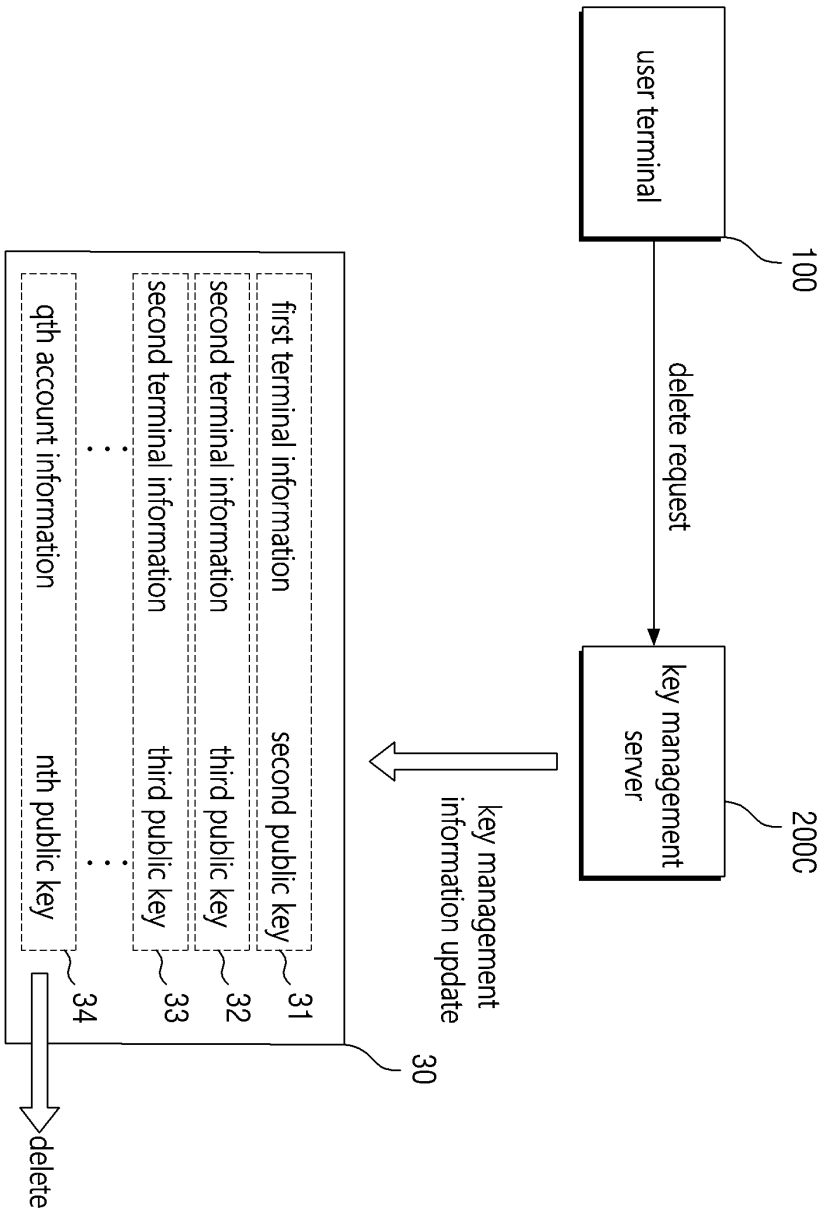

user terminal
100
delete request
key management server
200C
key management information update
30
first terminal information
second public key
31
second terminal information
third public key
32
second terminal information
third public key
33
qth account information
nth public key
34
delete

FIG. 30

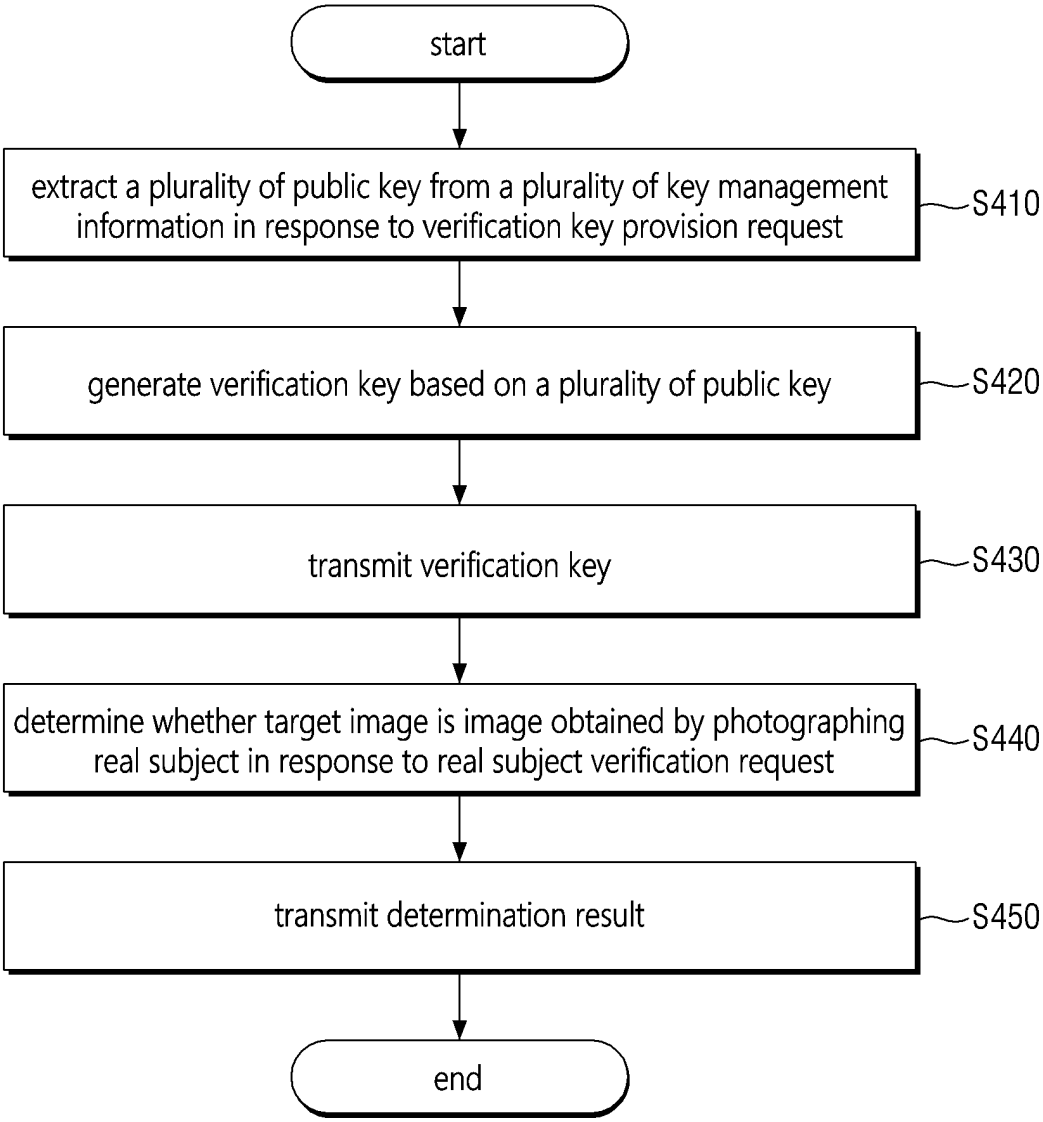

start
extract a plurality of public key from a plurality of key management information in response to verification key provision request
S410
generate verification key based on a plurality of public key
S420
transmit verification key
S430
determine whether target image is image obtained by photographing real subject in response to real subject verification request
S440
transmit determination result
S450
end

FIG. 31

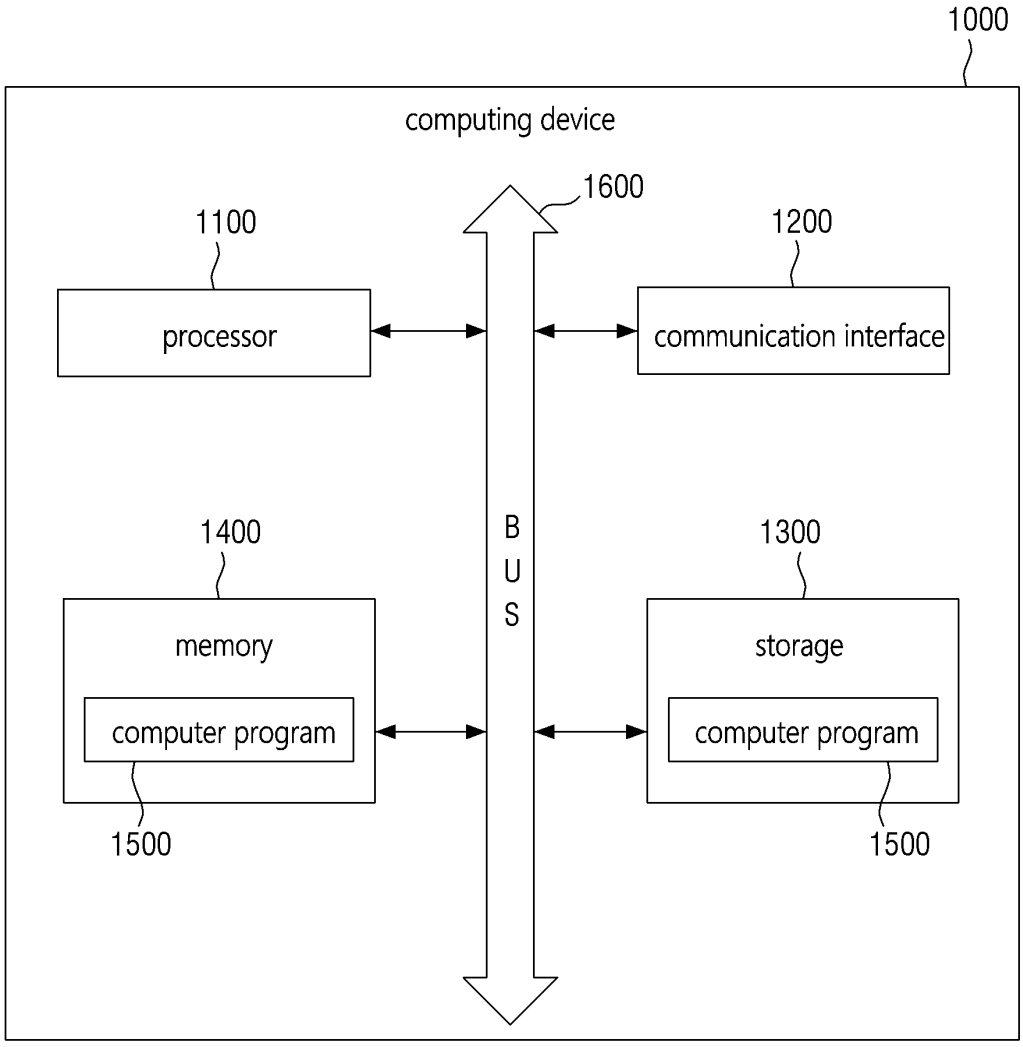

1000
computing device
1600
1100
1200
processor
communication interface
B
U
S
1400
1300
memory
storage
computer program
computer program
1500
1500

FIG. 32