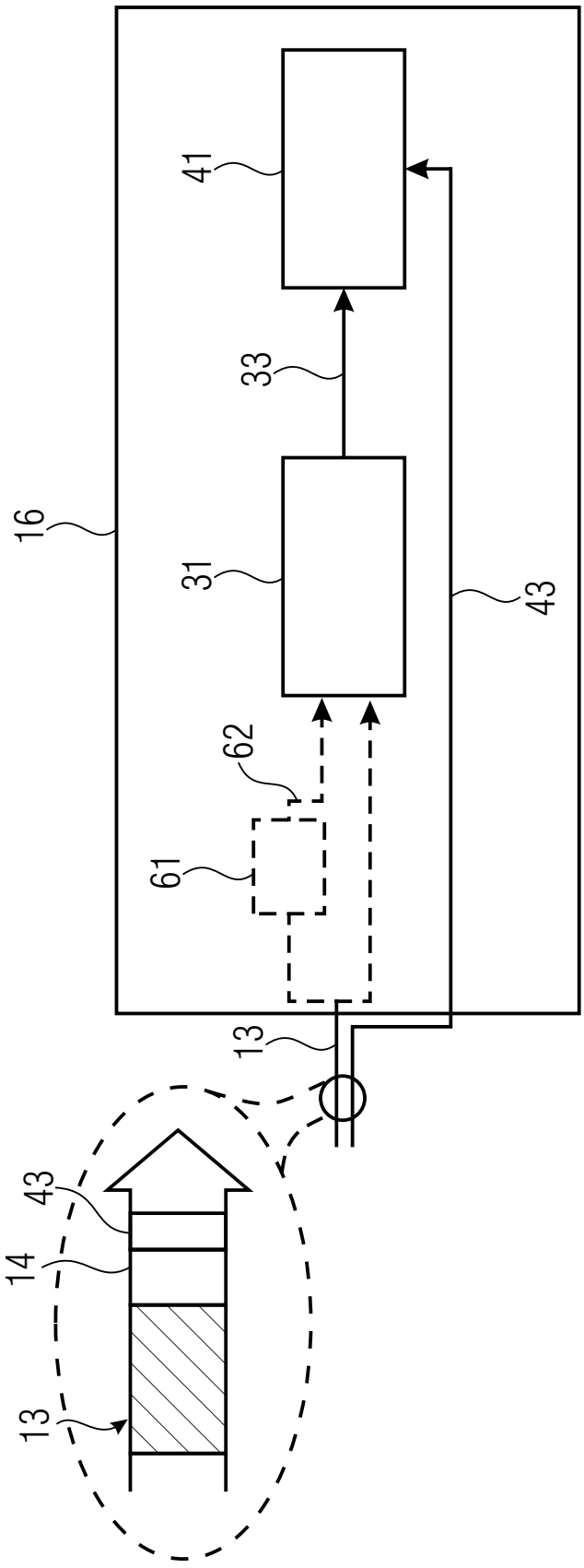

Fig. 1

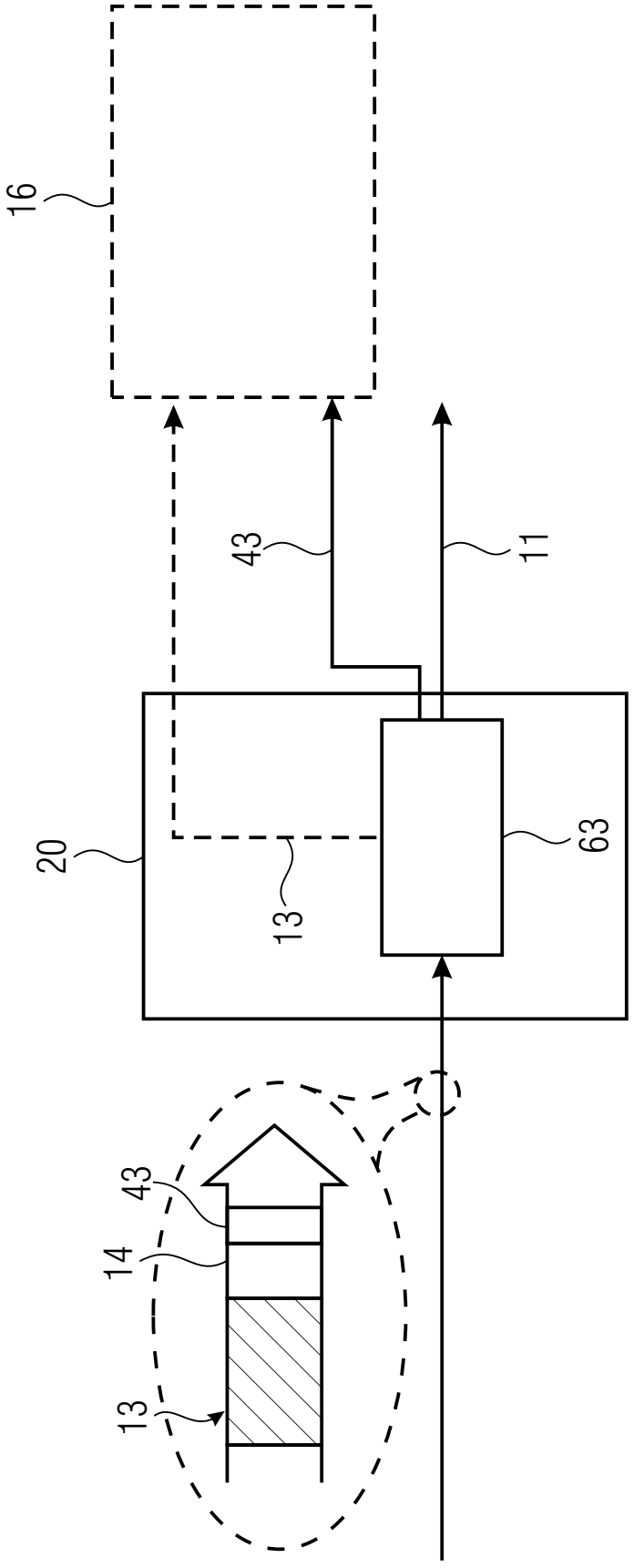

Fig. 2

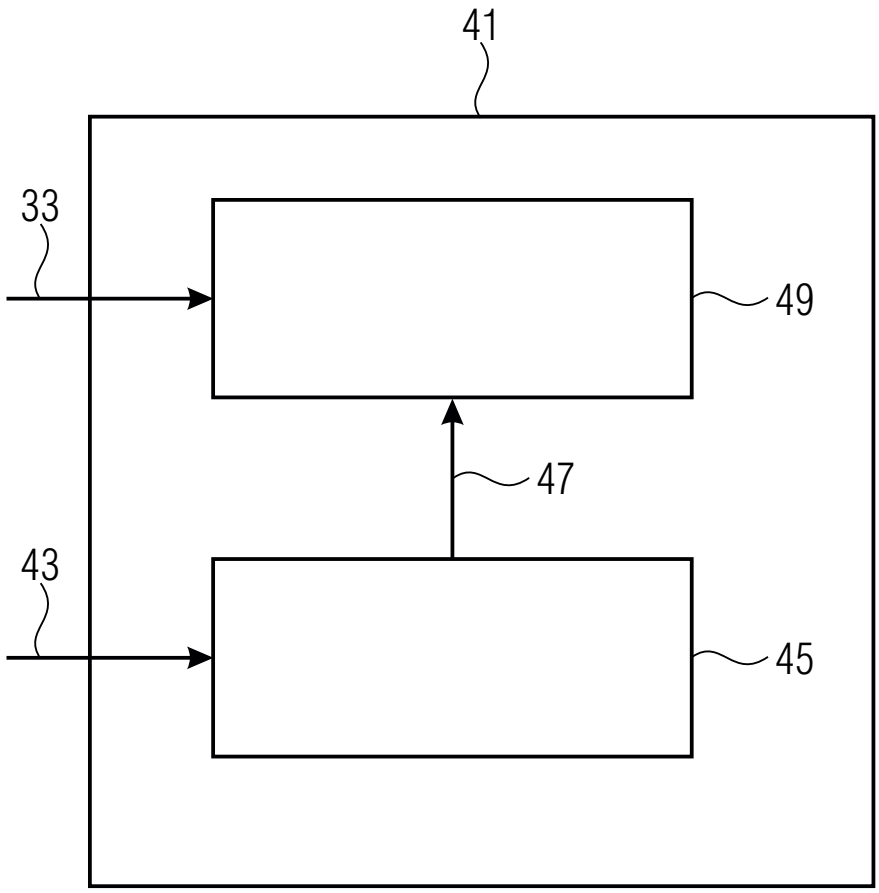

Fig. 3

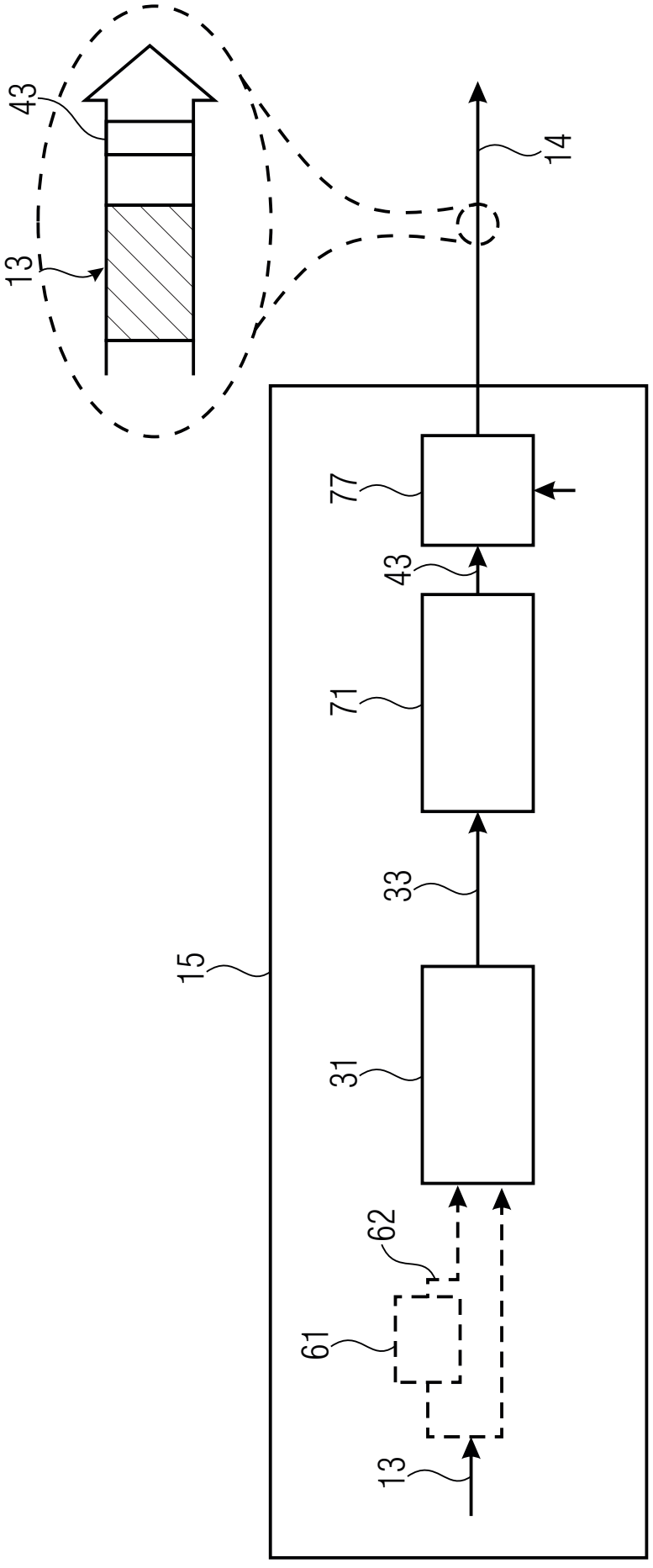

Fig. 4

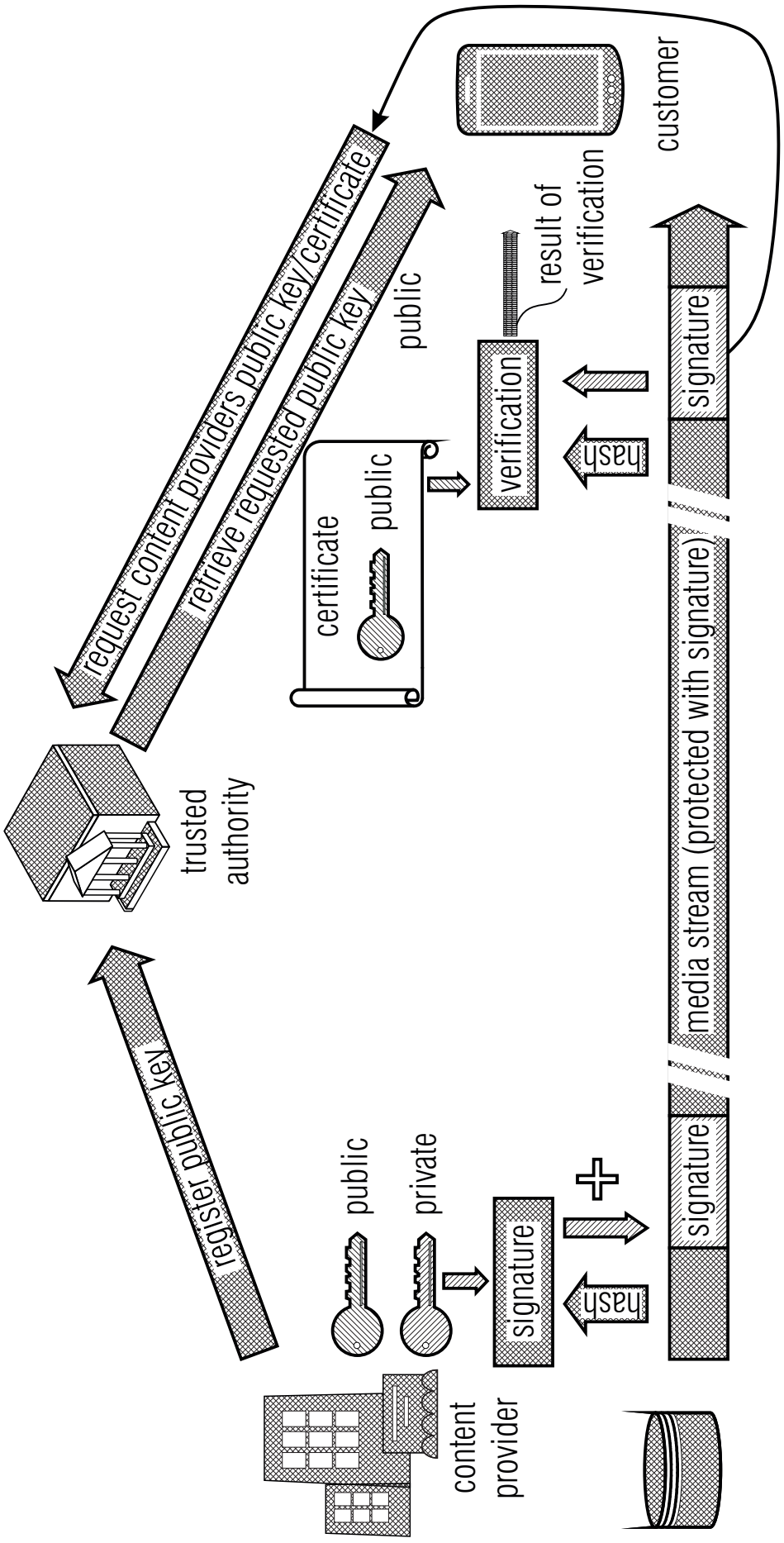
request content providers public key/certificate
retrieve requested public key
public
result of verification
customer
certificate
public
verification
hash
signature
trusted authority
media stream (protected with signature)
register public key
public
private
signature
hash
signature
content provider

Fig. 5

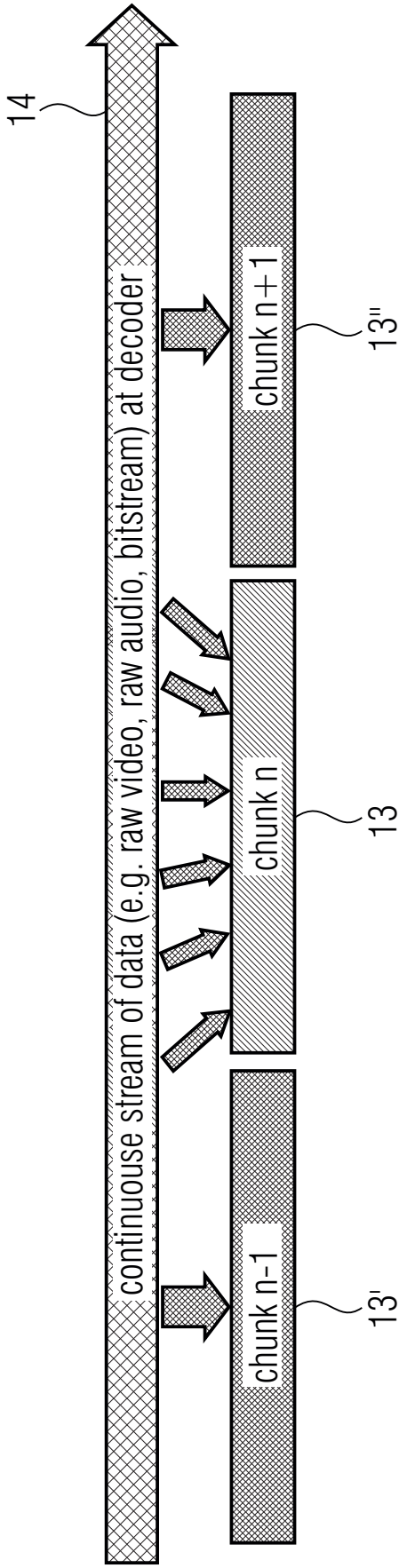
14
continuouse stream of data (e.g. raw video, raw audio, bitstream) at decoder
chunk n-1
13'
chunk n
13
chunk n+1
13''

Fig. 6A

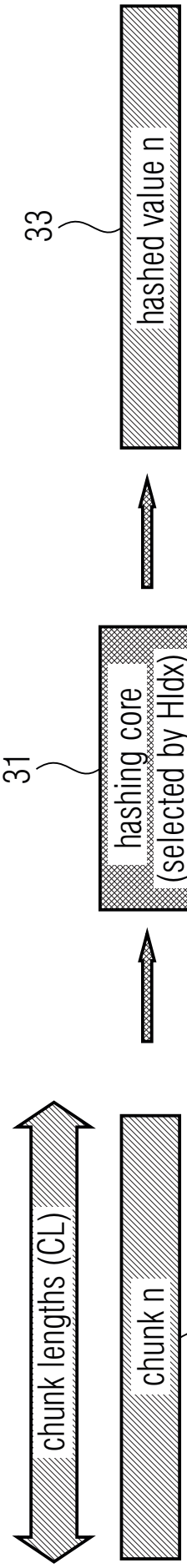
chunk lengths (CL)
chunk n
13
hashing core
(selected by Hldx)
31
hashed value n
33

Fig. 6B

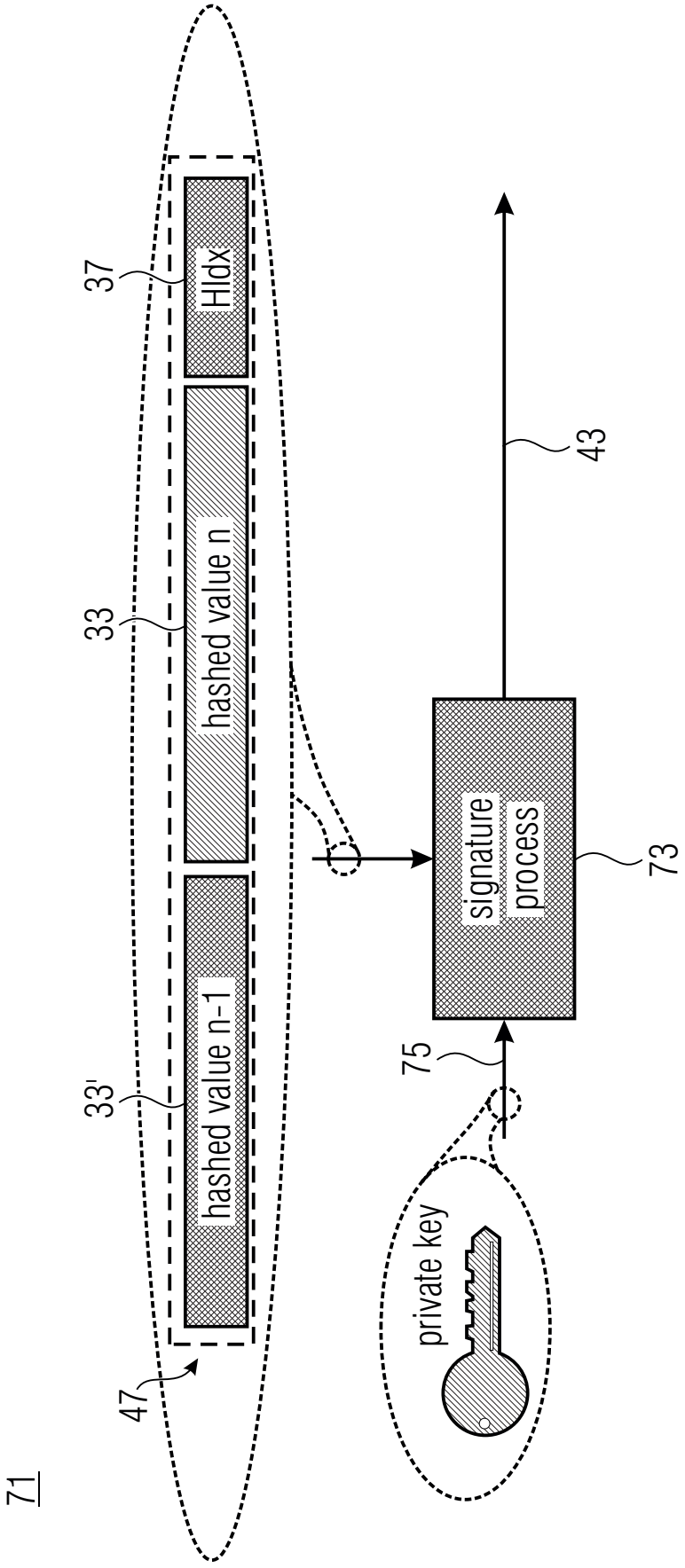
71
47
37
Hldx
33
hashed value n
33'
hashed value n-1
43
signature process
73
75
private key

Fig. 6C

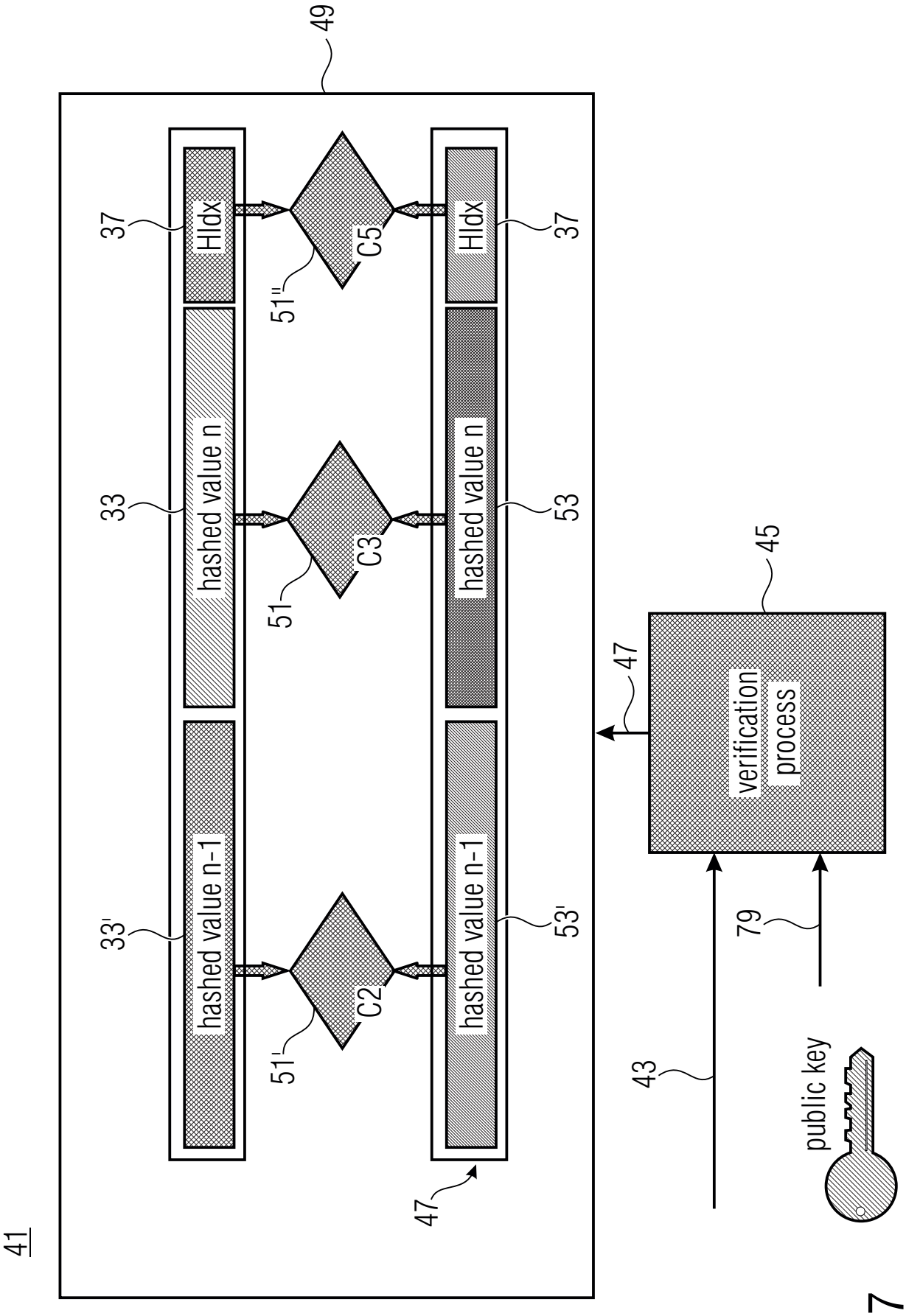
41
49
37
HIdx
C5
51''
HIdx
37
33
hashed value n
C3
51
hashed value n
53
33'
hashed value n-1
C2
51'
hashed value n-1
53'
47
47
45
verification process
43
79
public key

Fig. 7

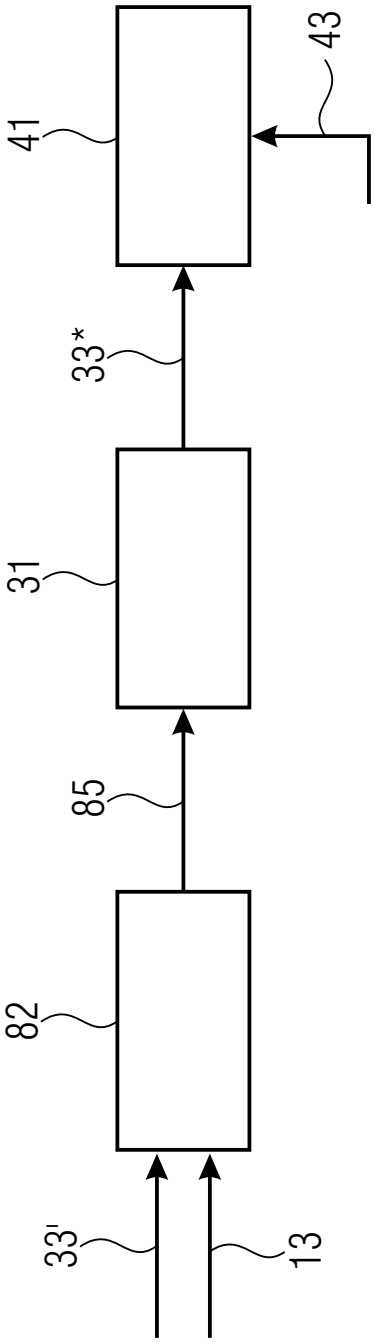

Fig. 8

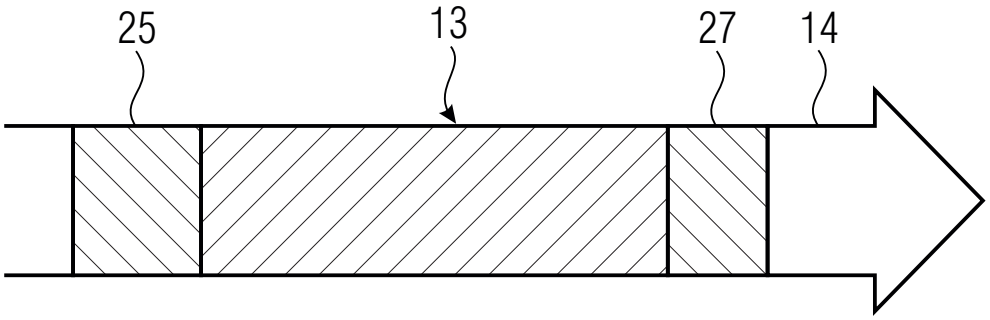

Fig. 9A

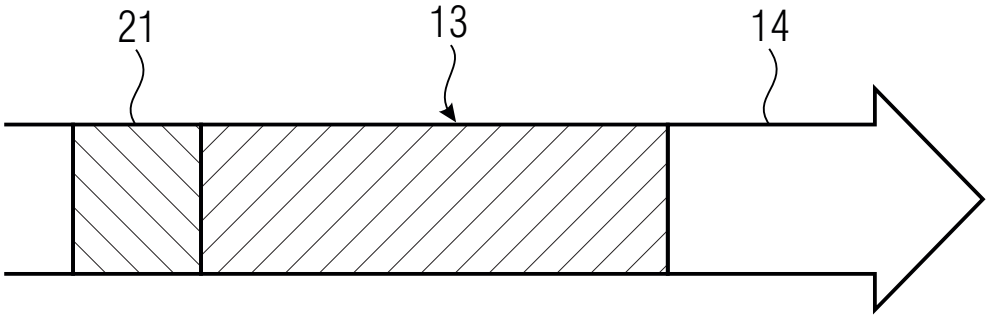

Fig. 9B

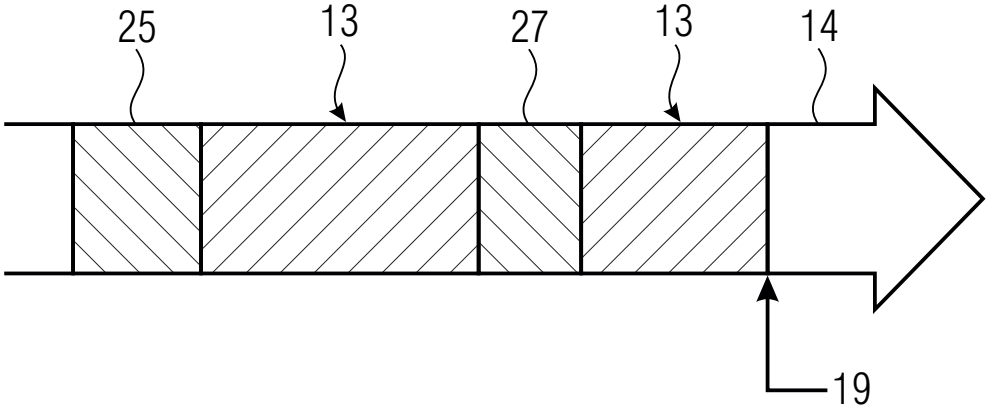

Fig. 9C

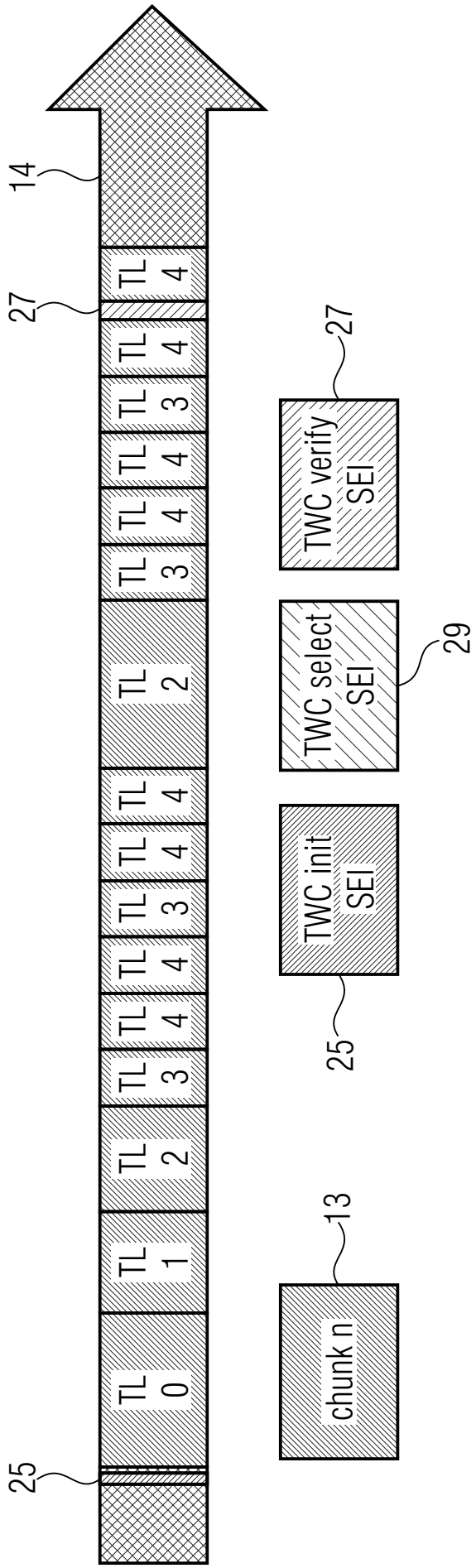

Fig. 10A

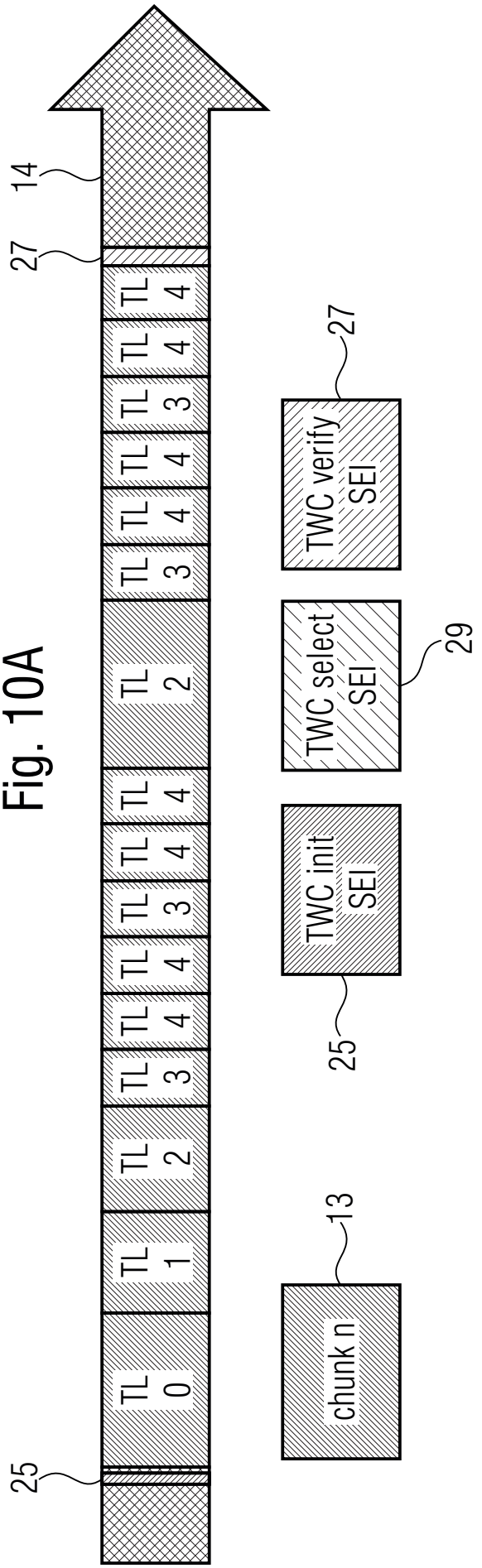

Fig. 10B

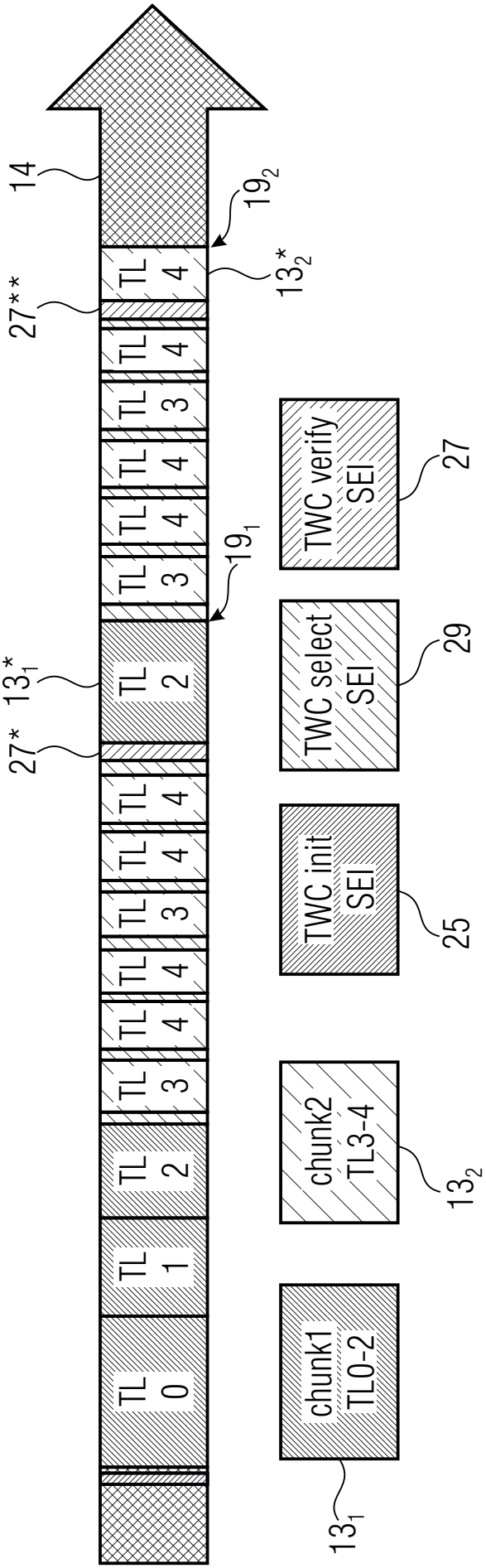

Fig. 11A

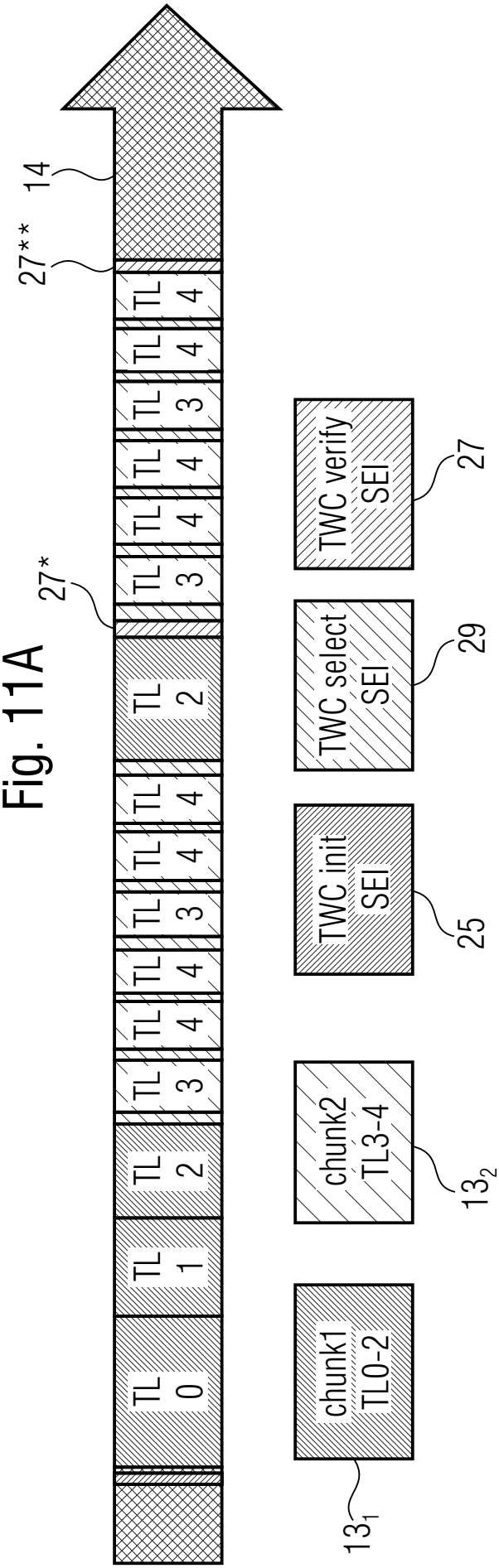

Fig. 11B

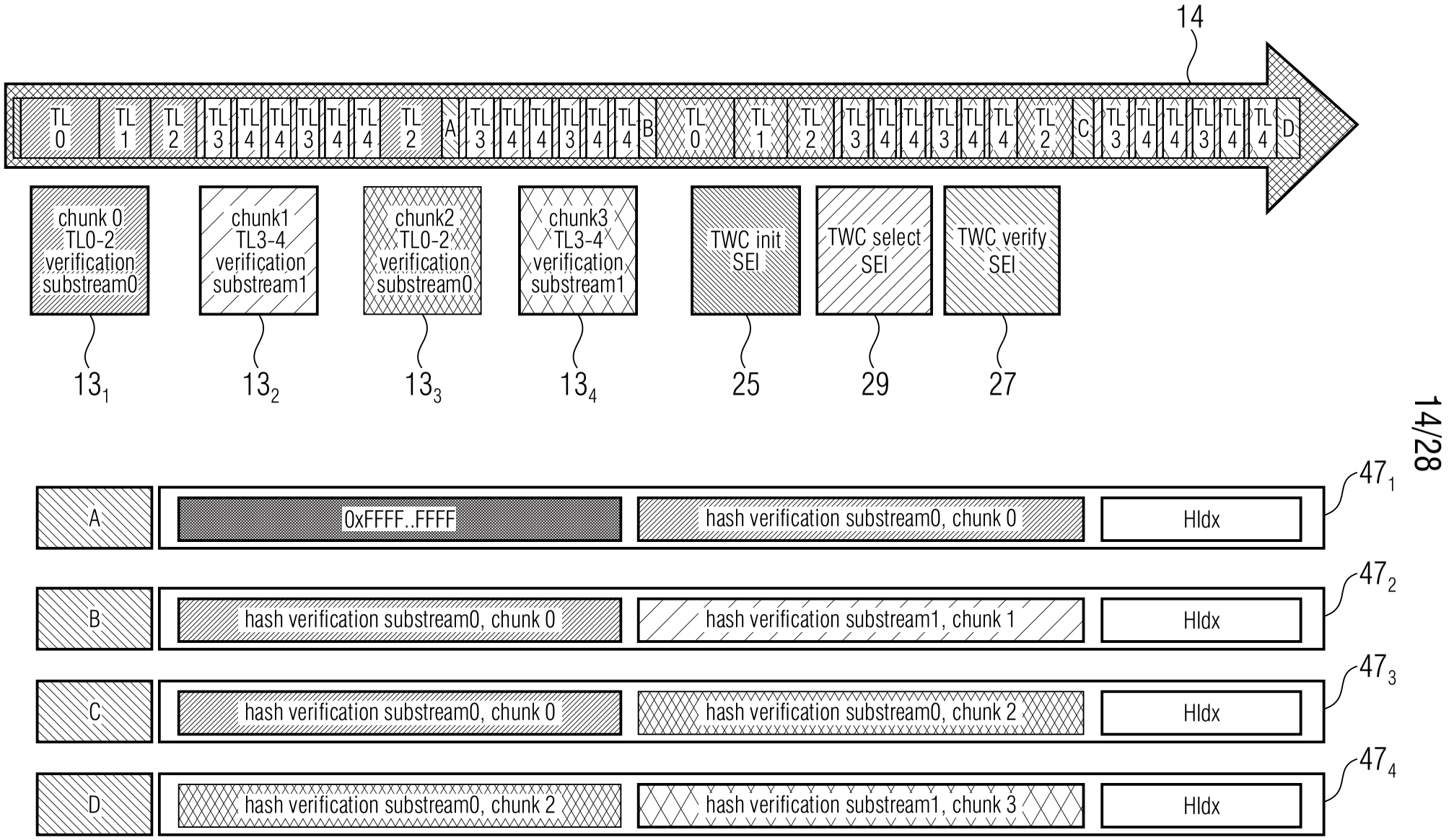
14
TL 0
TL 1
TL 2
TL 3
TL 4
A
B
C
D
chunk 0 TL0-2 verification substream0
chunk1 TL3-4 verification substream1
chunk2 TL0-2 verification substream0
chunk3 TL3-4 verification substream1
TWC init SEI
TWC select SEI
TWC verify SEI
13 1
13 2
13 3
13 4
25
29
27
14/28
47 1
47 2
47 3
47 4
0xFFFF..FFFF
hash verification substream0, chunk 0
hash verification substream1, chunk 1
hash verification substream0, chunk 2
hash verification substream1, chunk 3
HIdx

Fig. 12



Fig. 13

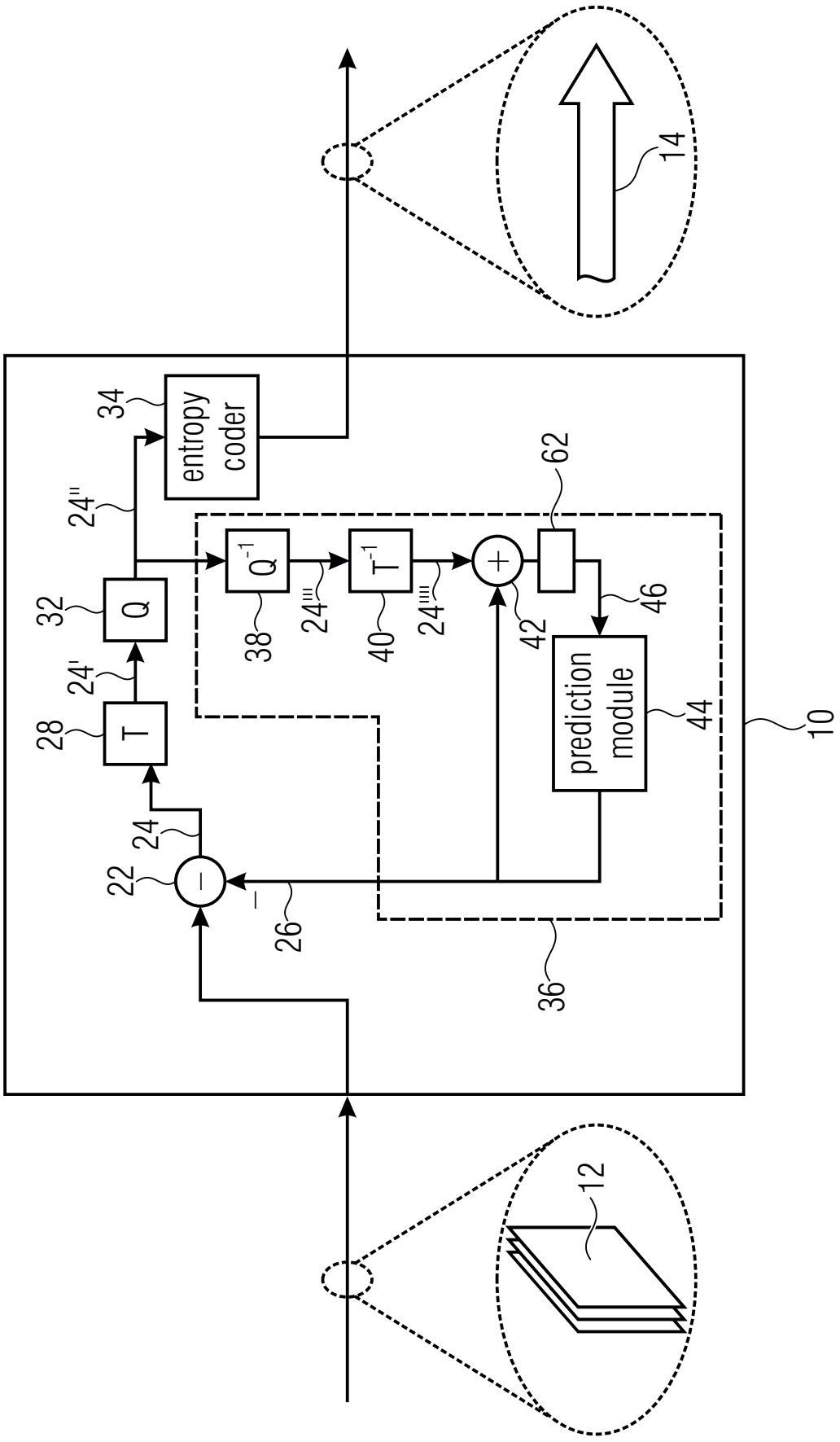
entropy coder
34
24''
32
Q
24'
28
T
24
22
26
38
Q^{-1}
24'''
40
T^{-1}
24''''
42
62
46
prediction module
44
36
10
12
14

Fig. 14

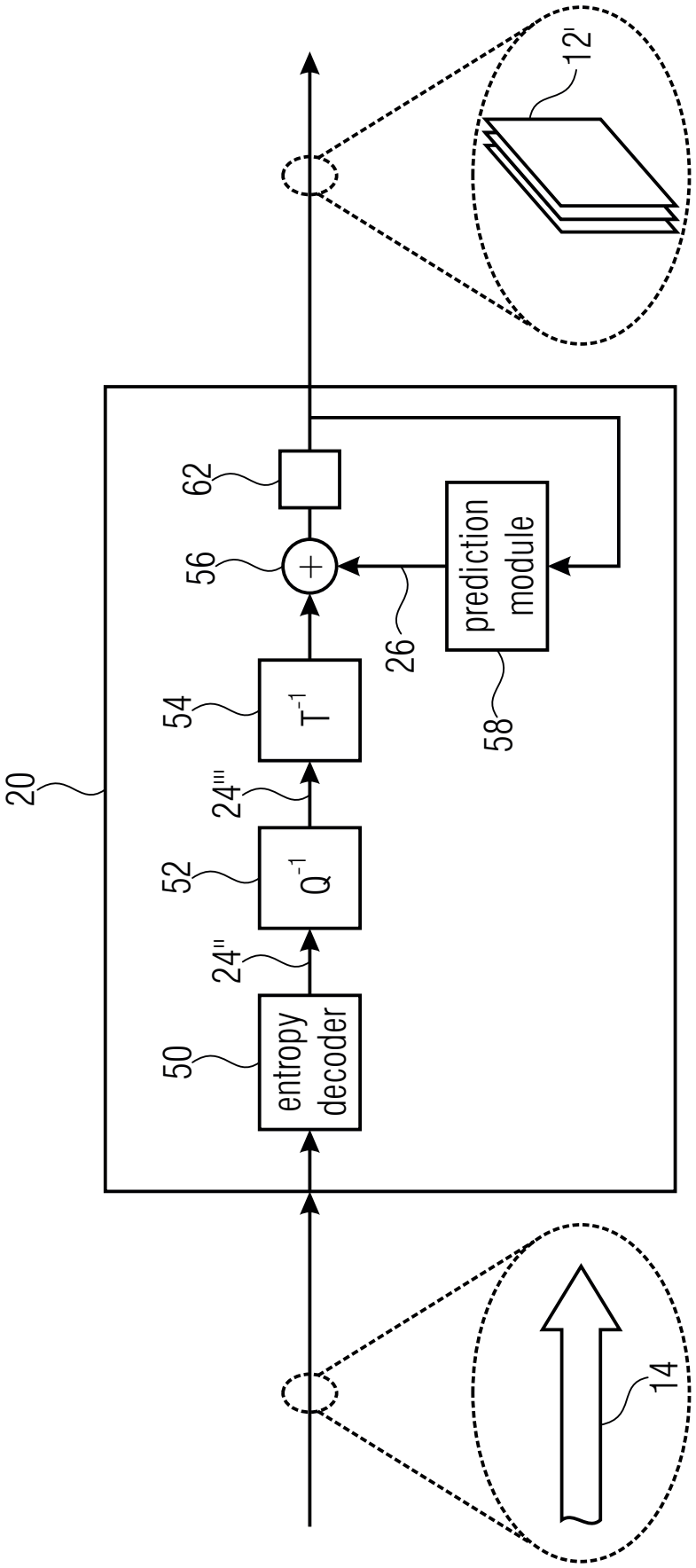
12'
62
56
prediction module
26
58
54
T^{-1}
24'''
52
Q^{-1}
24''
50
entropy decoder
20
14

Fig. 15

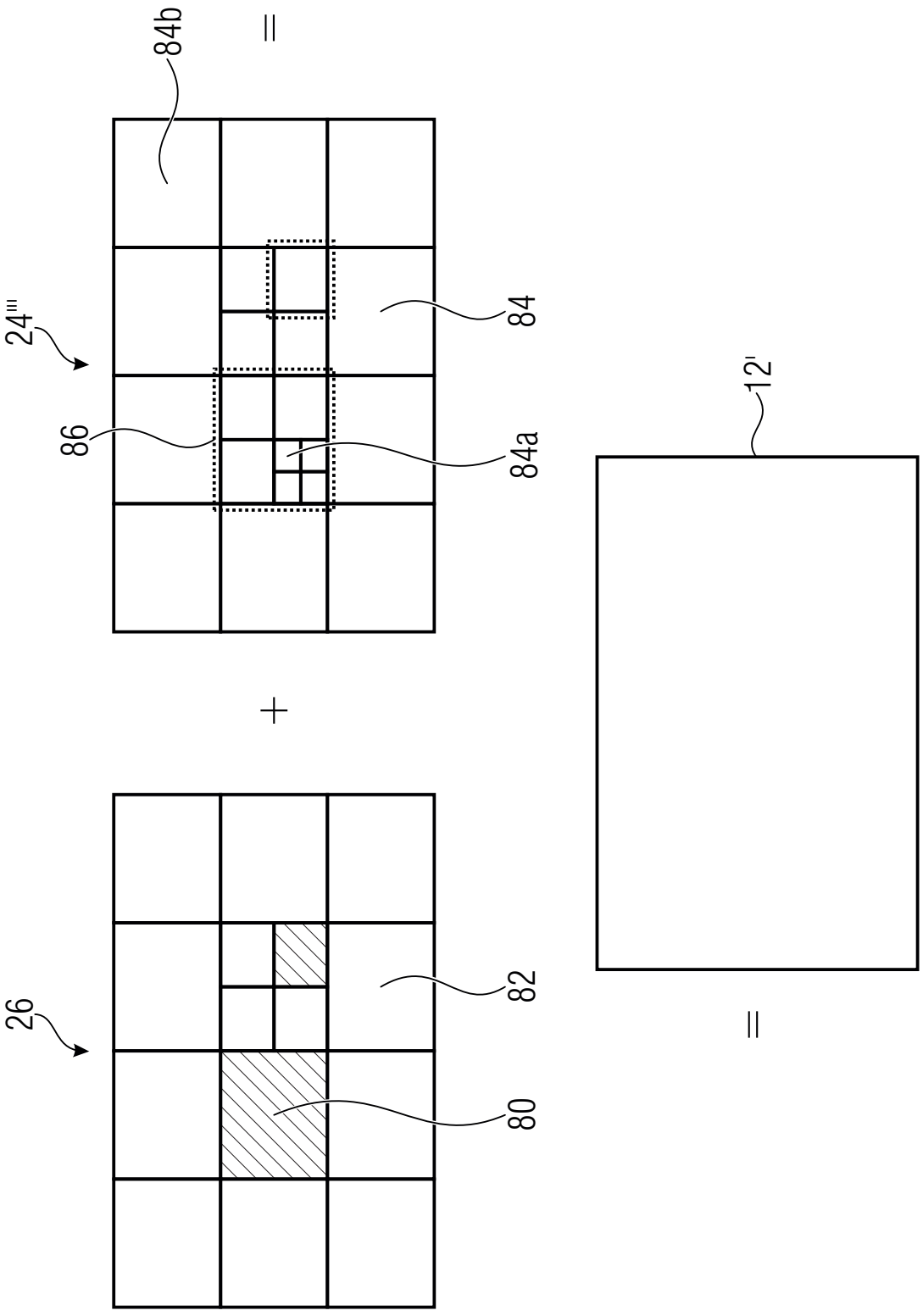

Fig. 16

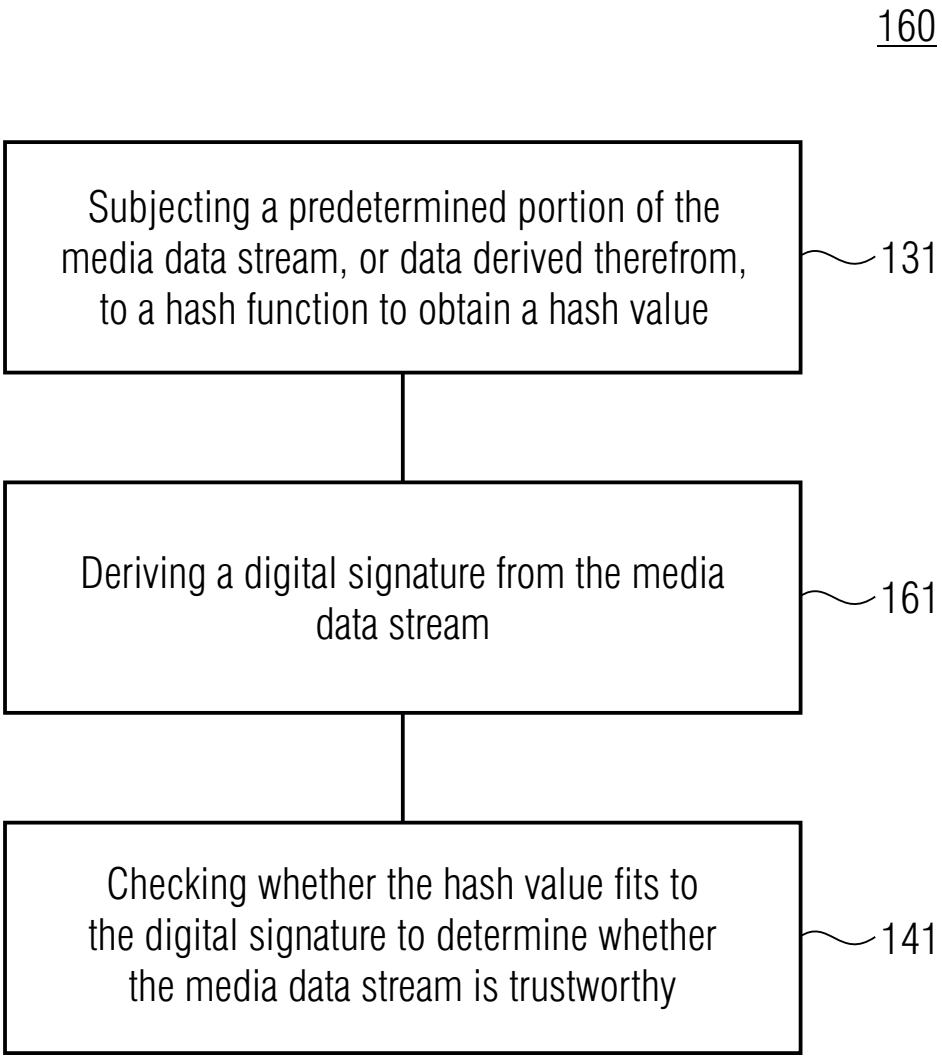
160
Subjecting a predetermined portion of the media data stream, or data derived therefrom, to a hash function to obtain a hash value
131
Deriving a digital signature from the media data stream
161
Checking whether the hash value fits to the digital signature to determine whether the media data stream is trustworthy
141

Fig. 17

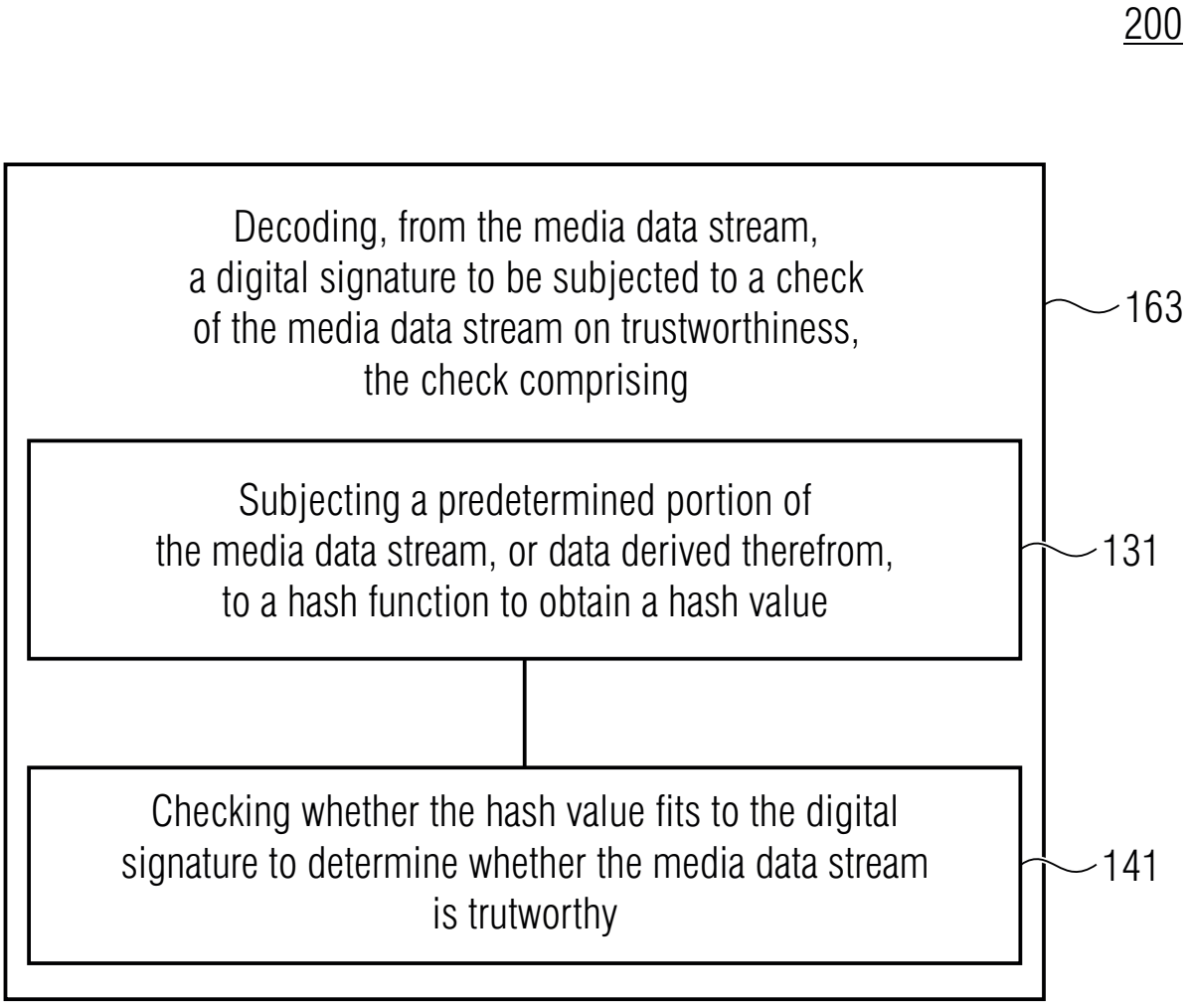
200
Decoding, from the media data stream, a digital signature to be subjected to a check of the media data stream on trustworthiness, the check comprising
163
Subjecting a predetermined portion of the media data stream, or data derived therefrom, to a hash function to obtain a hash value
131
Checking whether the hash value fits to the digital signature to determine whether the media data stream is trutworthy
141

Fig. 18

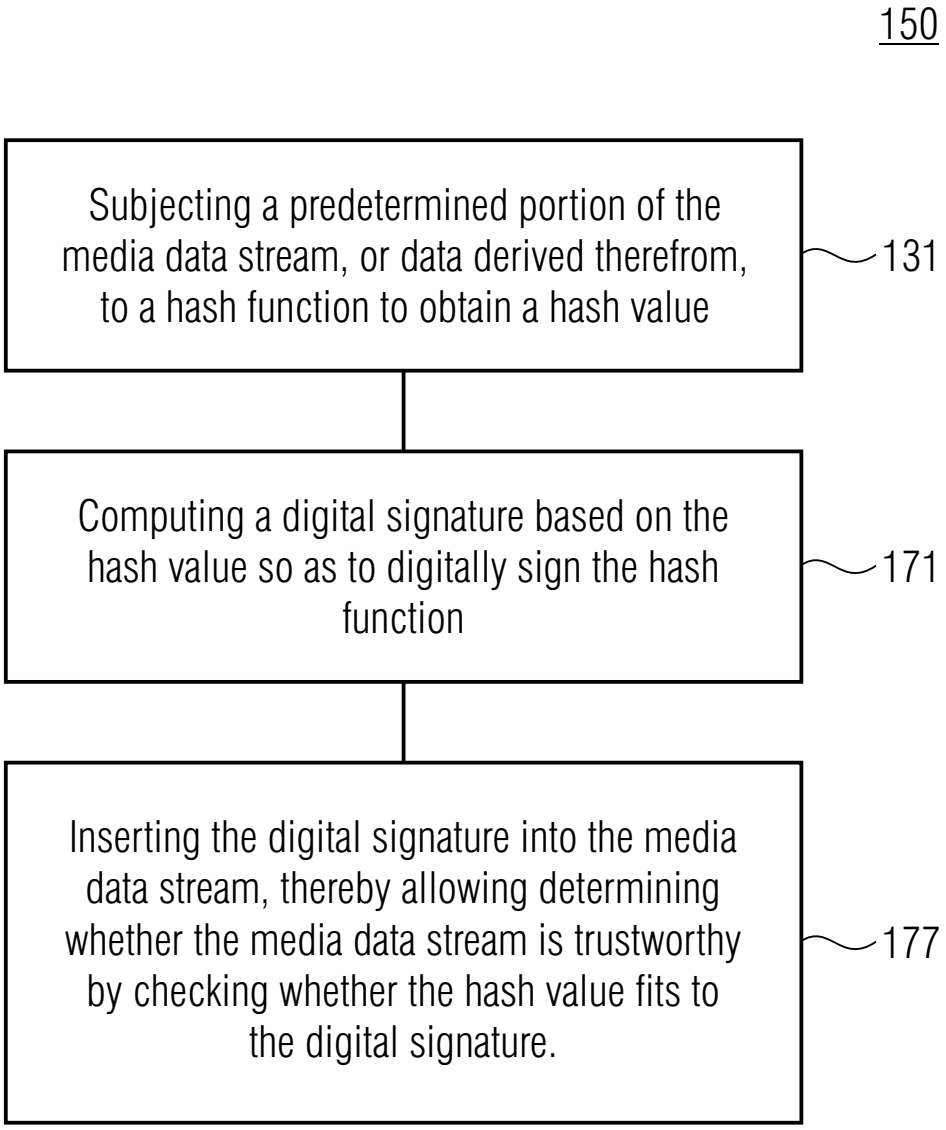
150
Subjecting a predetermined portion of the media data stream, or data derived therefrom, to a hash function to obtain a hash value
131
Computing a digital signature based on the hash value so as to digitally sign the hash function
171
Inserting the digital signature into the media data stream, thereby allowing determining whether the media data stream is trustworthy by checking whether the hash value fits to the digital signature.
177

Fig. 19

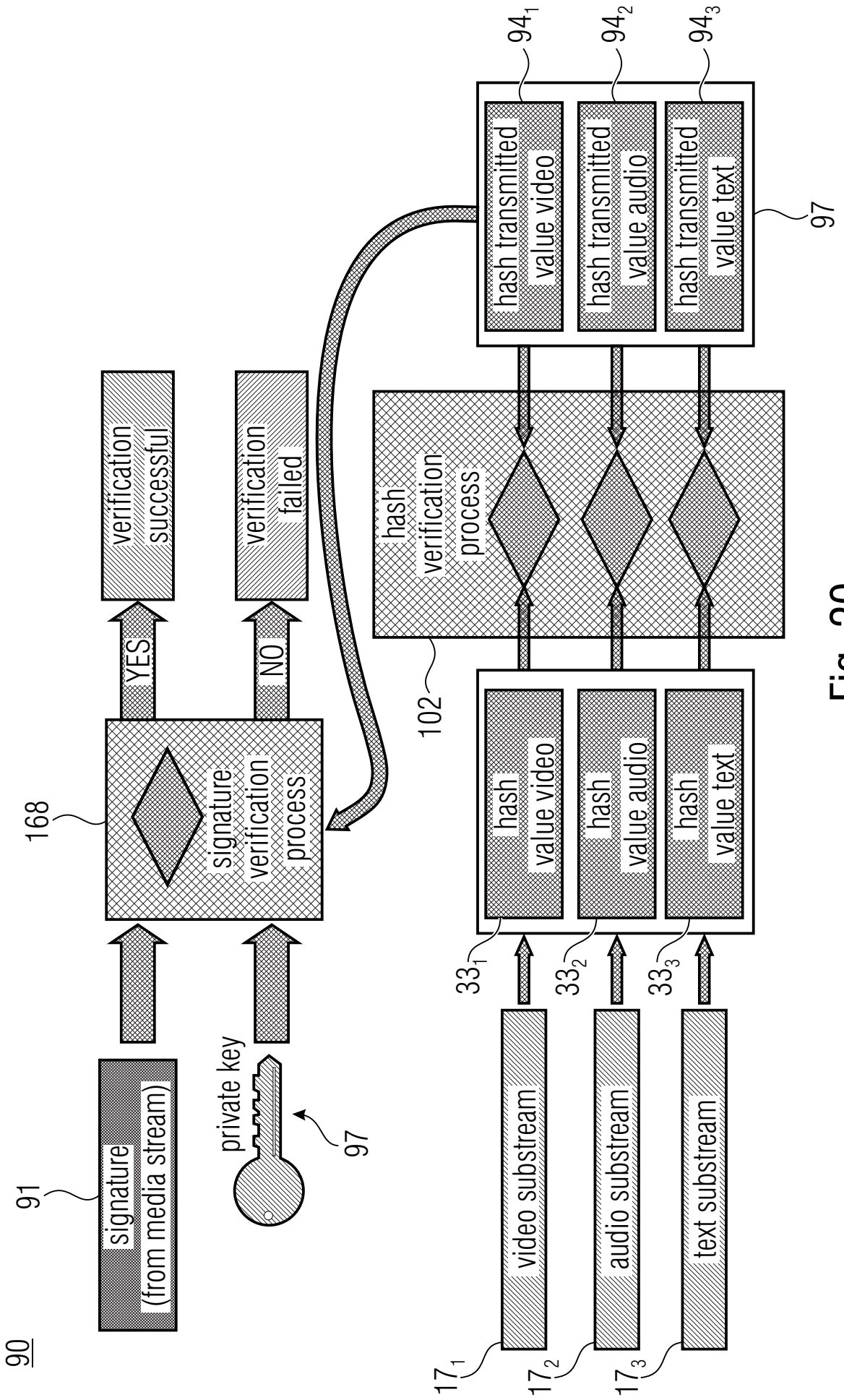
90
91
signature
(from media stream)
private key
97
168
signature verification process
YES
NO
verification successful
verification failed
17_1
17_2
17_3
video substream
audio substream
text substream
33_1
33_2
33_3
hash value video
hash value audio
hash value text
102
hash verification process
94_1
94_2
94_3
hash transmitted value video
hash transmitted value audio
hash transmitted value text
97

Fig. 20

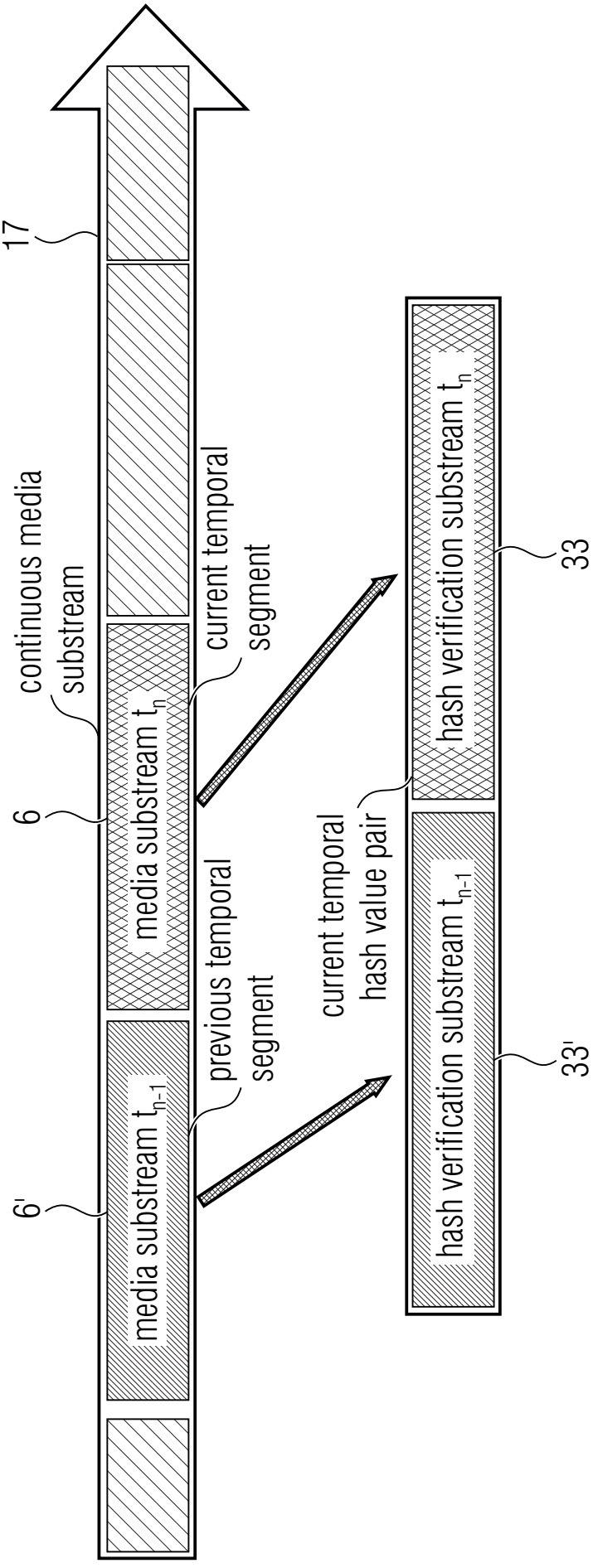
17
continuous media substream
6
media substream t_n
current temporal segment
previous temporal segment
6'
media substream t_{n-1}
current temporal hash value pair
hash verification substream t_n
33
33'
hash verification substream t_{n-1}

Fig. 21

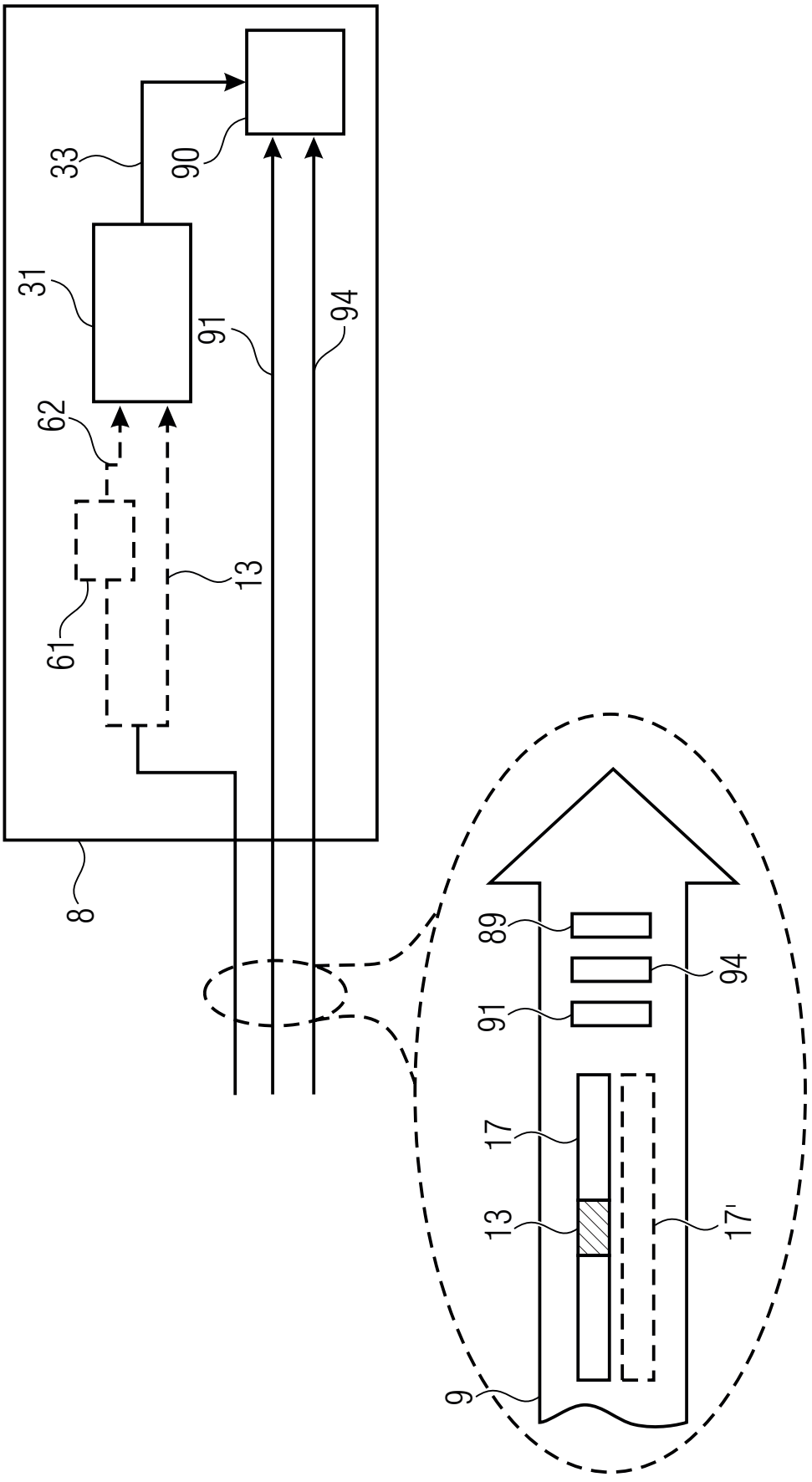

Fig. 22

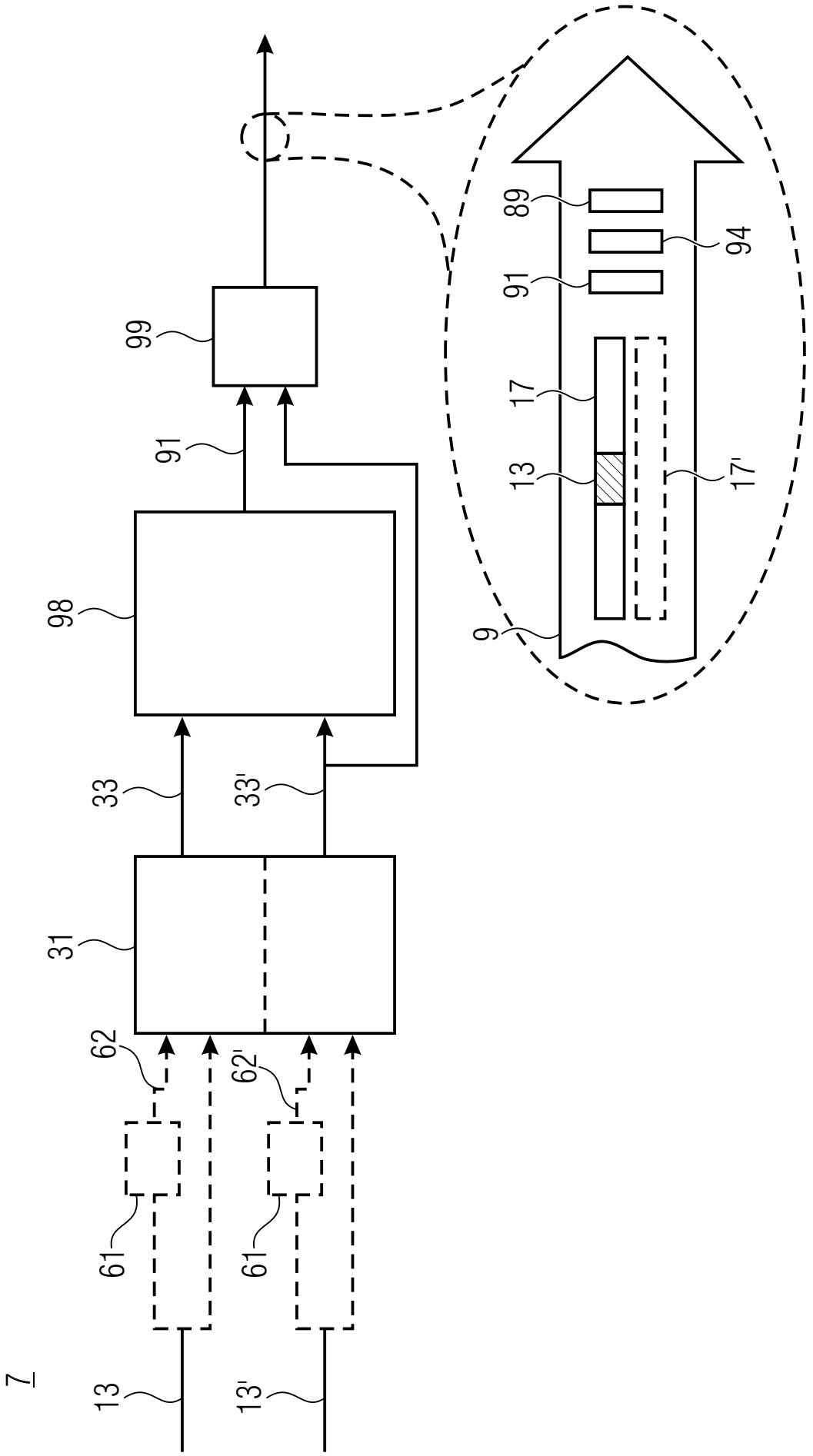

Fig. 23

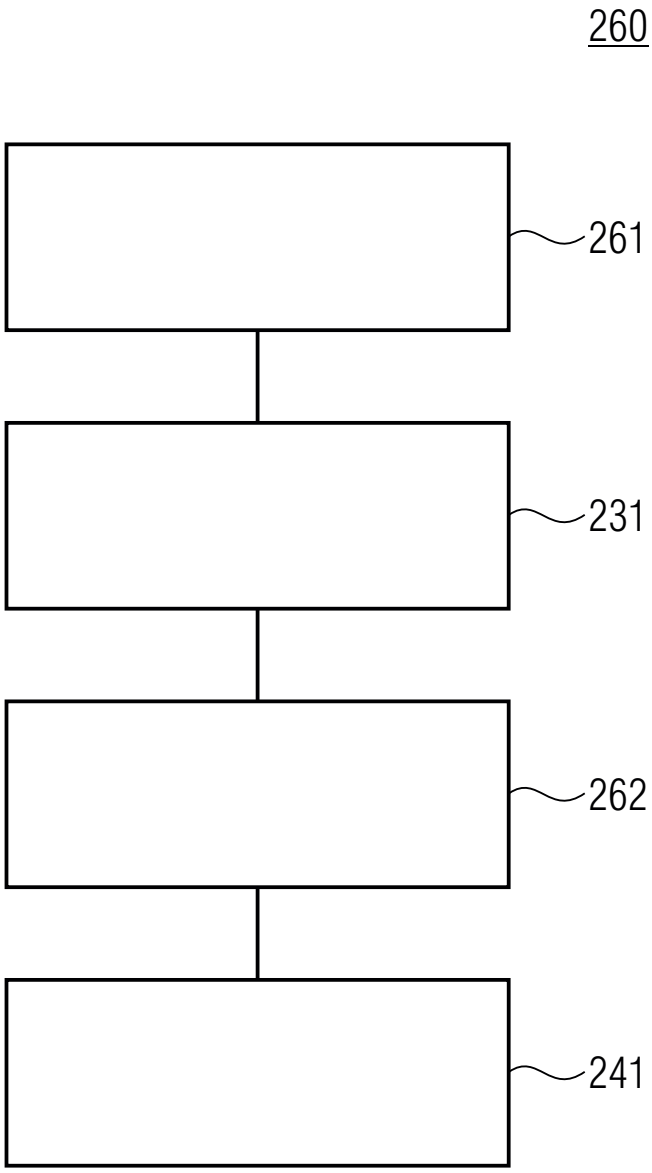

Fig. 24

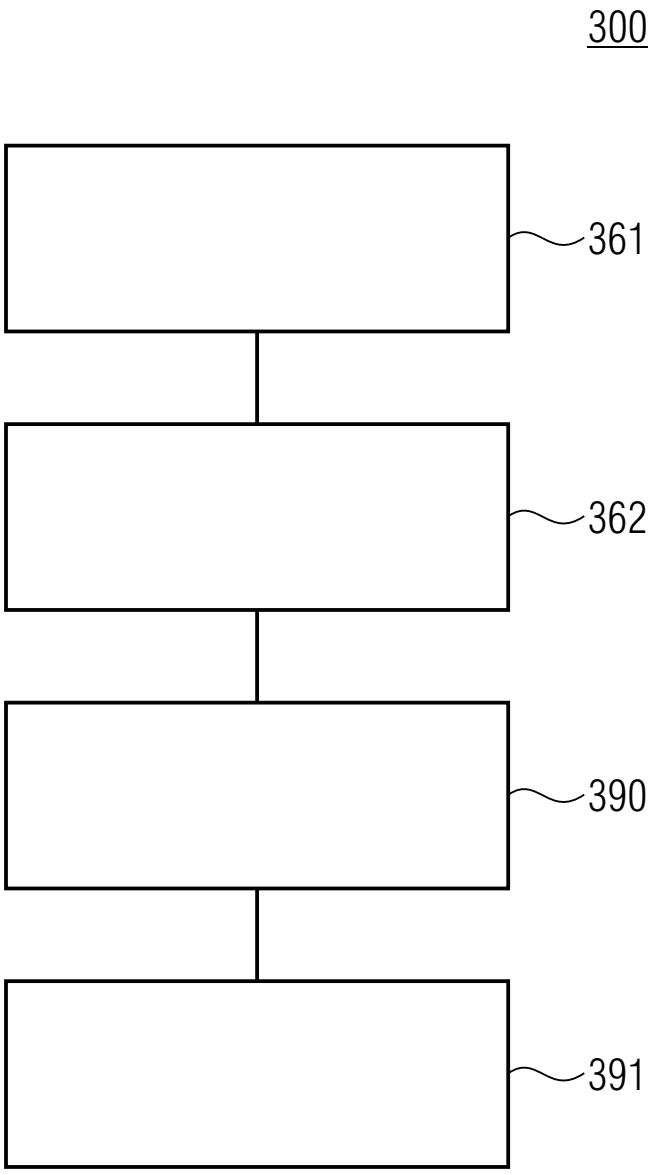

Fig. 25

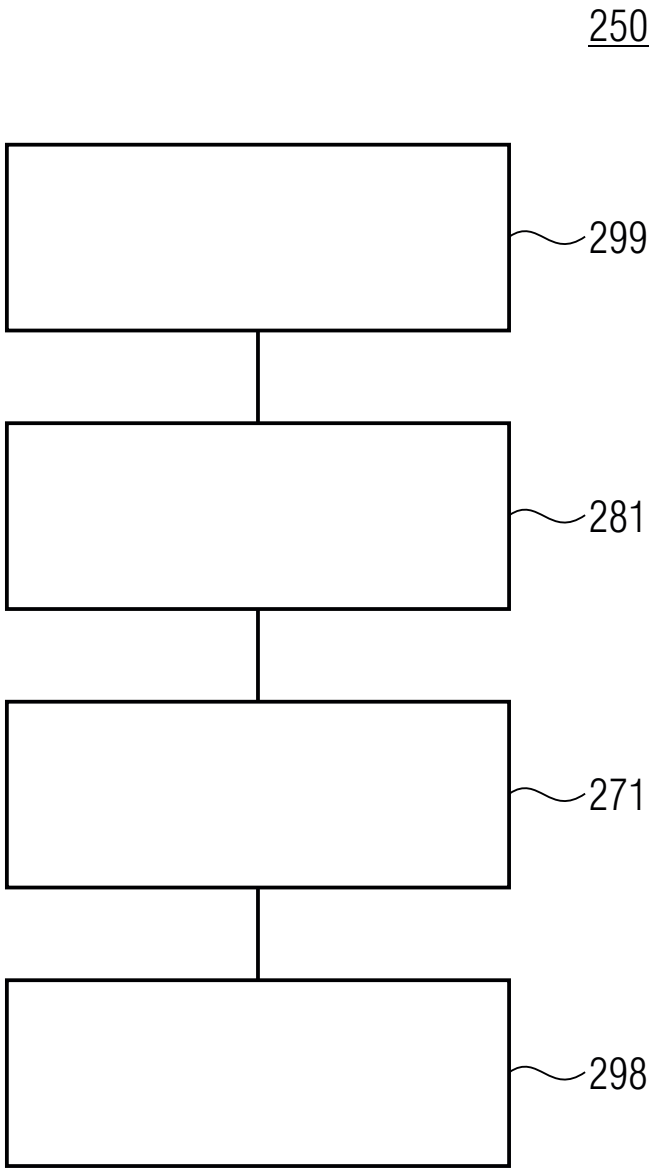

Fig. 26