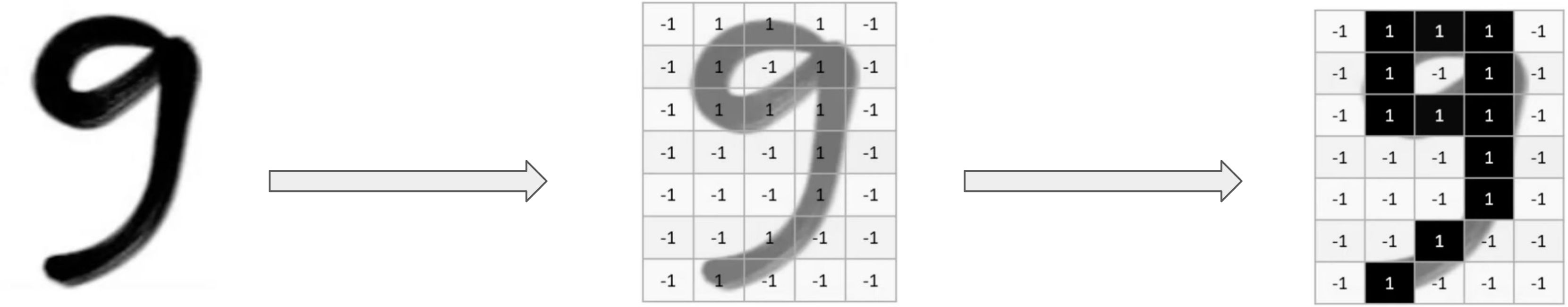
CYBER W207
Applied Machine Learning for Cybersecurity

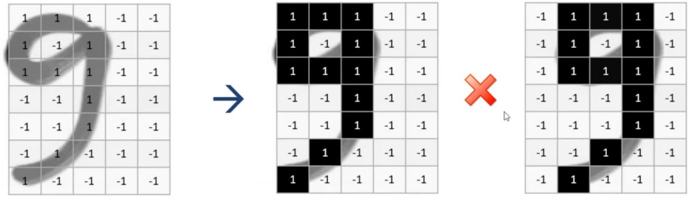
Week 10
Live Session Slides



-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

Location shifted



1	1	1	-1	-1
1	-1	1	-1	-1
1	1	1	-1	-1
-1	-1	1	-1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1
1	-1	-1	-1	-1

1	1	1	-1	-1
1	-1	1	-1	-1
1	1	1	-1	-1
-1	-1	1	-1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1
1	-1	-1	-1	-1

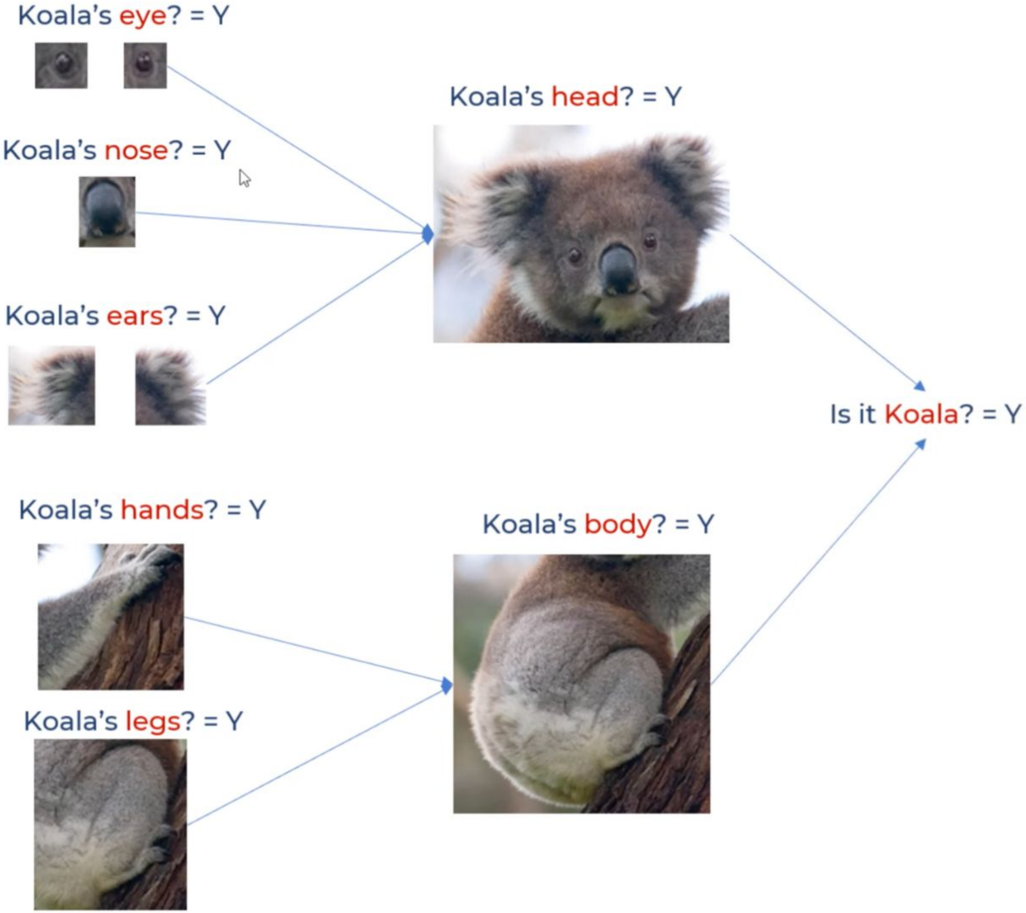
-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

Image size = 1920 x 1080 X 3

First layer neurons = 1920 x 1080 X 3 ~ 6 million

Hidden layer neurons = Let’s say you keep it ~ 4 million

Weights between input and hidden layer = 6 mil * 4 mil
= 24 million



Koala's eye? = Y

Koala's nose? = Y

Koala's ears? = Y

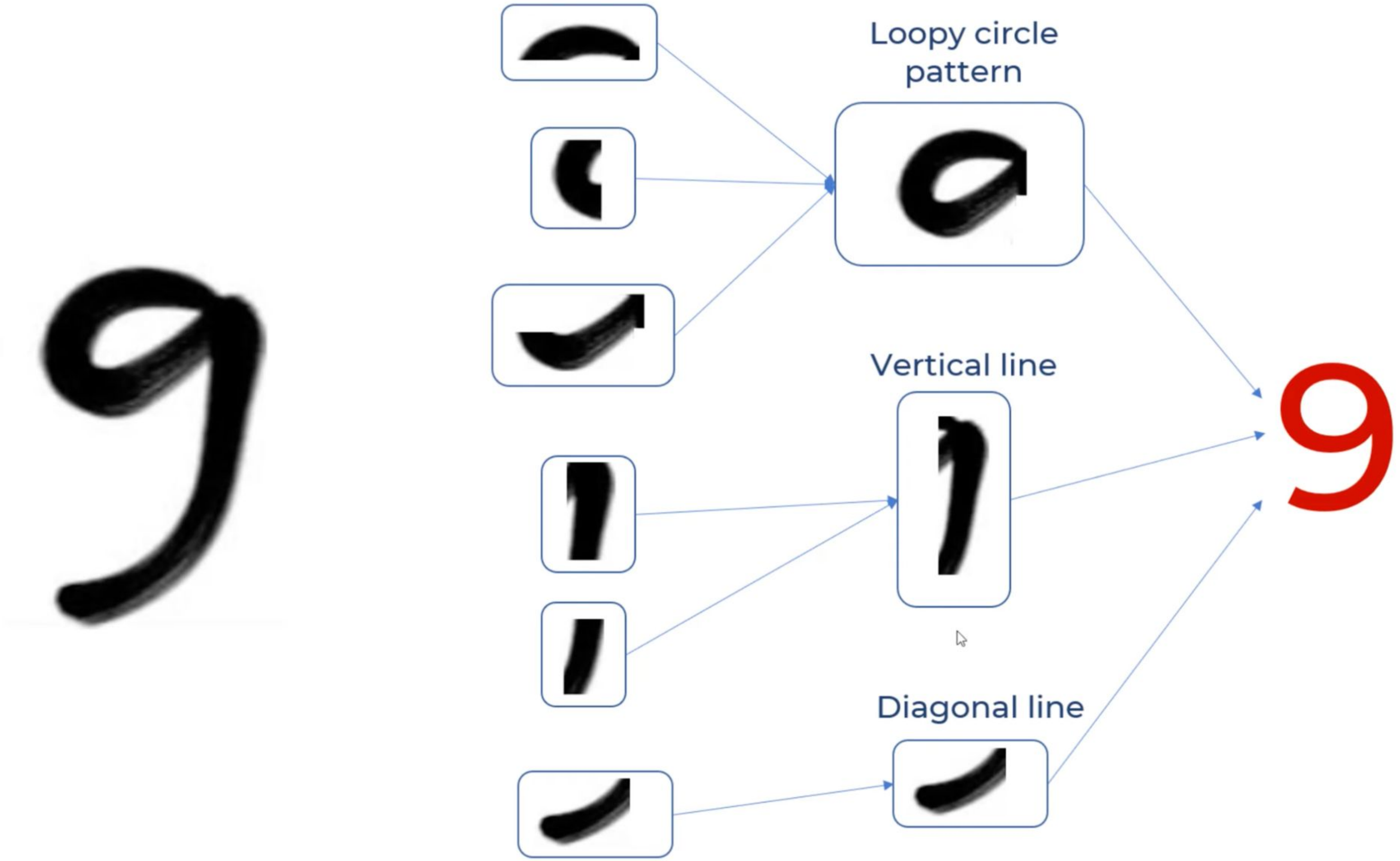
Koala's head? = Y

Koala's hands? = Y

Koala's legs? = Y

Koala's body? = Y

Is it Koala? = Y

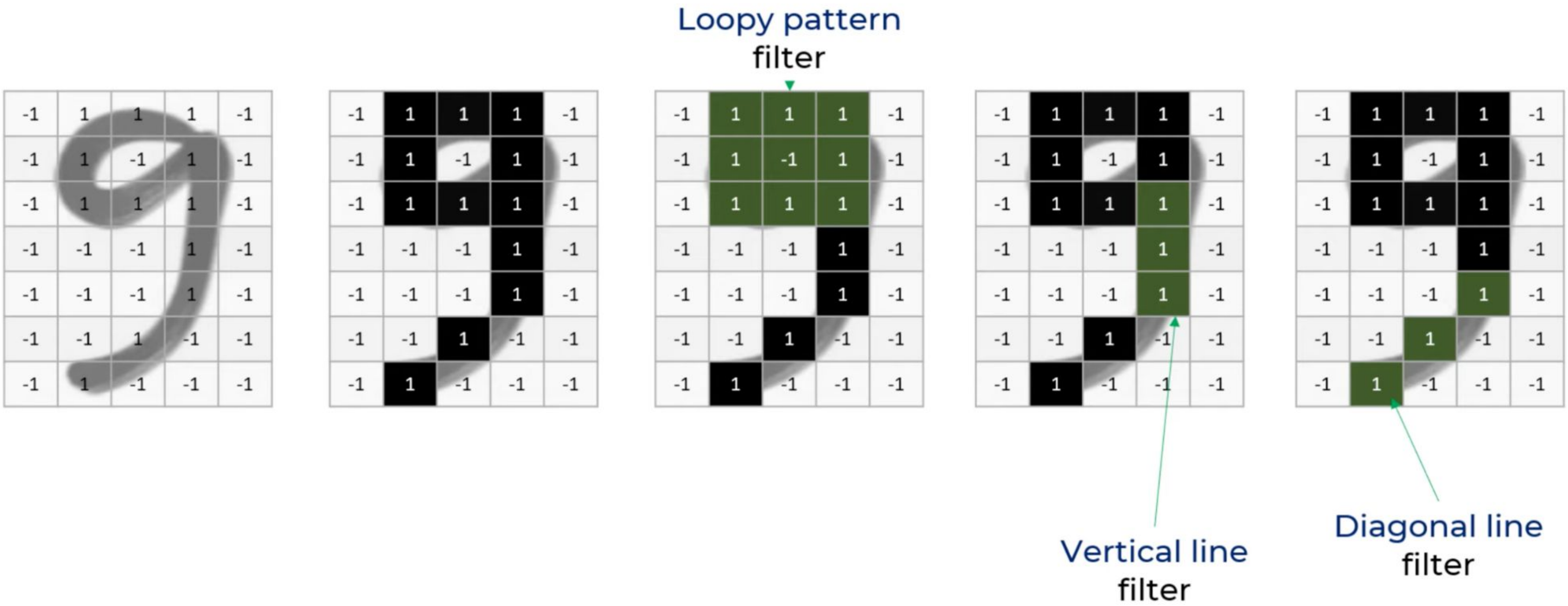


Loopy circle pattern

Vertical line

Diagonal line

9



Loopy pattern filter

Vertical line filter

Diagonal line filter

-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

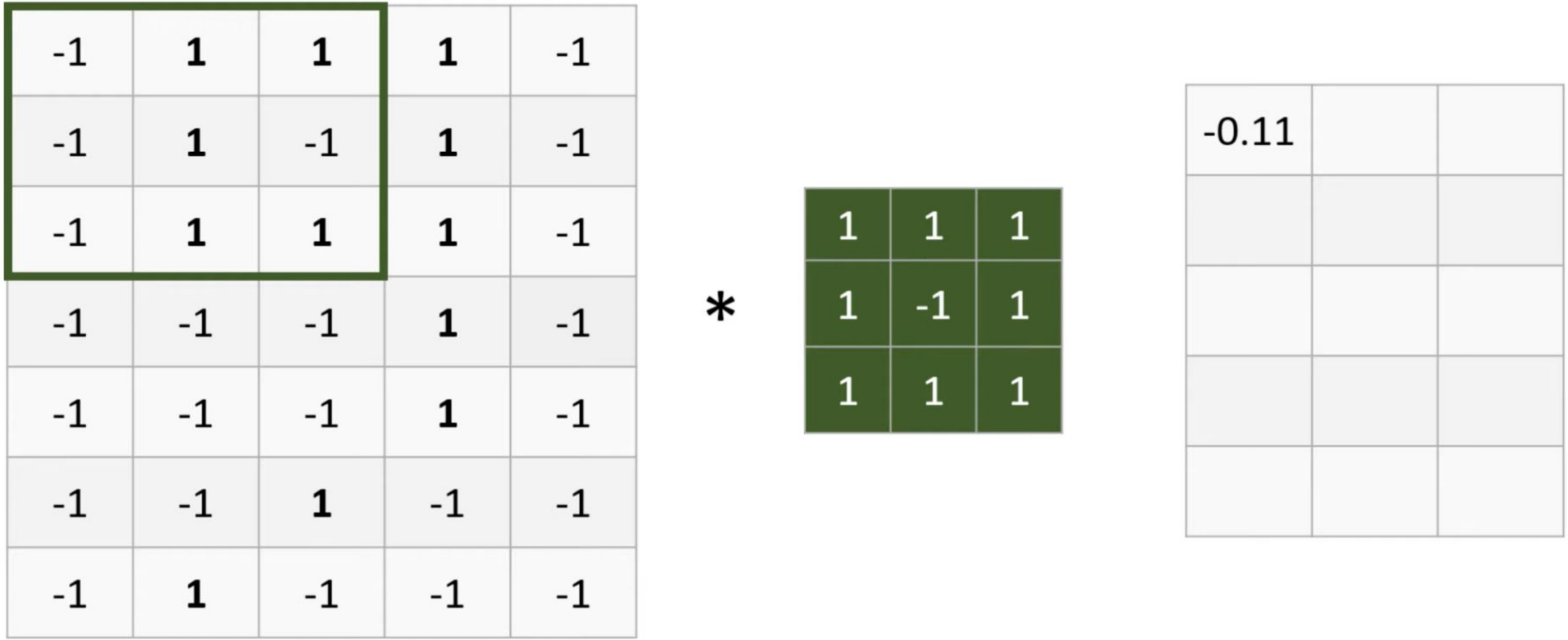
-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

$$-1+1+1-1-1-1-1+1+1 = -1 \rightarrow -1/9 = -0.11$$



-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

*

1	1	1
1	-1	1
1	1	1

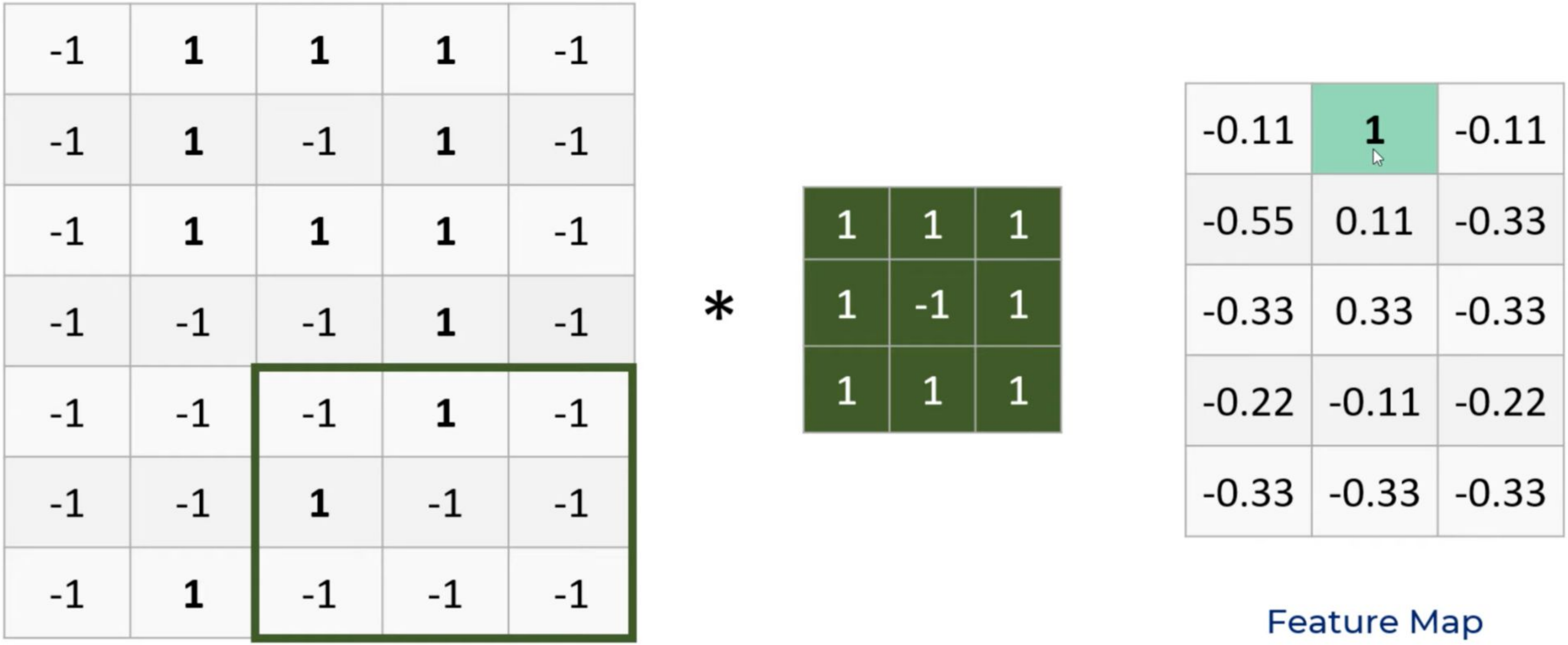
-0.11		

-1	**1**	**1**	**1**	-1
-1	**1**	-1	**1**	-1
-1	**1**	**1**	**1**	-1
-1	-1	-1	**1**	-1
-1	-1	-1	**1**	-1
-1	-1	**1**	-1	-1
-1	**1**	-1	-1	-1

*

1	1	1
1	-1	1
1	1	1

-0.11	1	-0.11
-0.55	0.11	-0.33



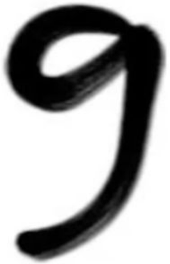
-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

*

1	1	1
1	-1	1
1	1	1

-0.11	1	-0.11
-0.55	0.11	-0.33
-0.33	0.33	-0.33
-0.22	-0.11	-0.22
-0.33	-0.33	-0.33

Feature Map



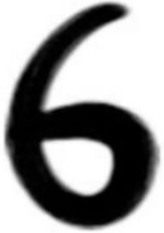
*

Loopy pattern detector

1	1	1
1	-1	1
1	1	1

=

	1	



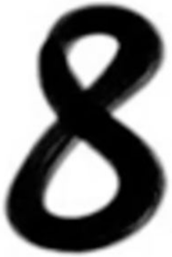
*

Loopy pattern detector

1	1	1
1	-1	1
1	1	1

=

	1	



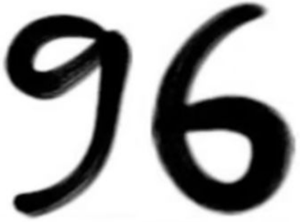
*

Loopy pattern detector

1	1	1
1	-1	1
1	1	1

=

	1	
	1	



*

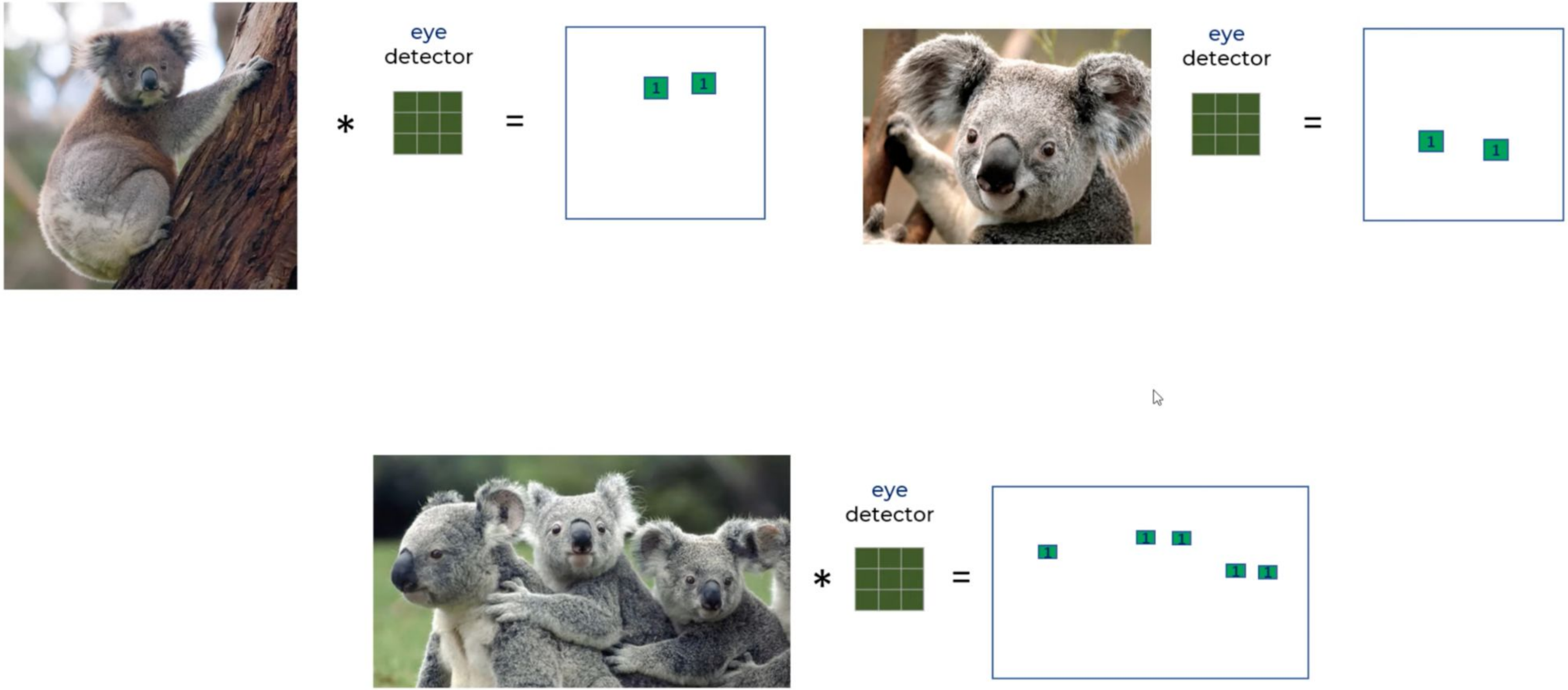
Loopy pattern detector

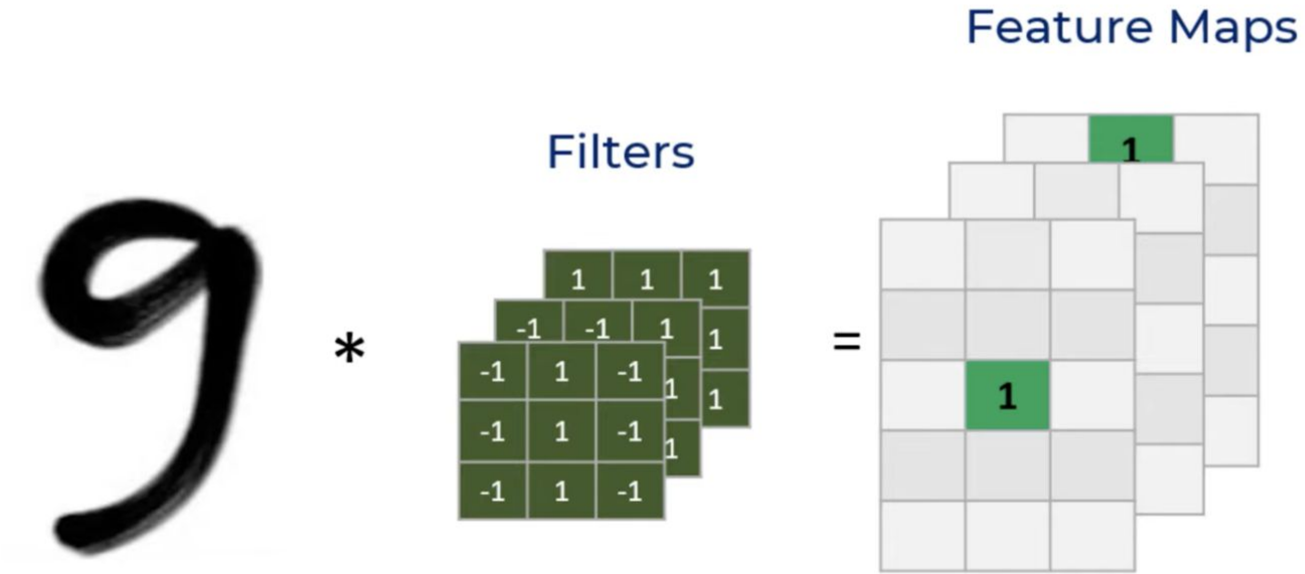
1	1	1
1	-1	1
1	1	1

=

	1			
			1	

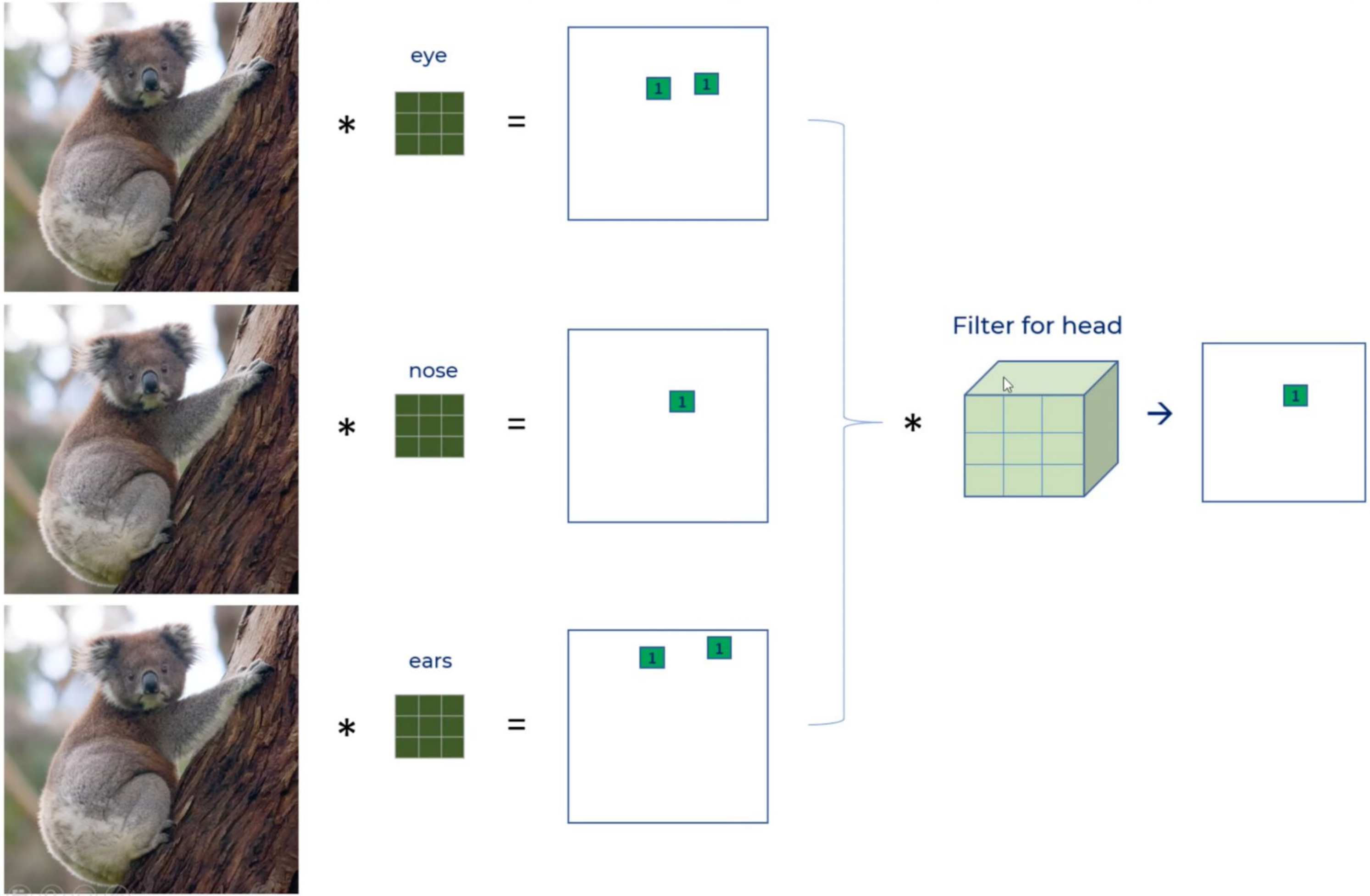
Location invariant: It can detect eyes in any location of the image

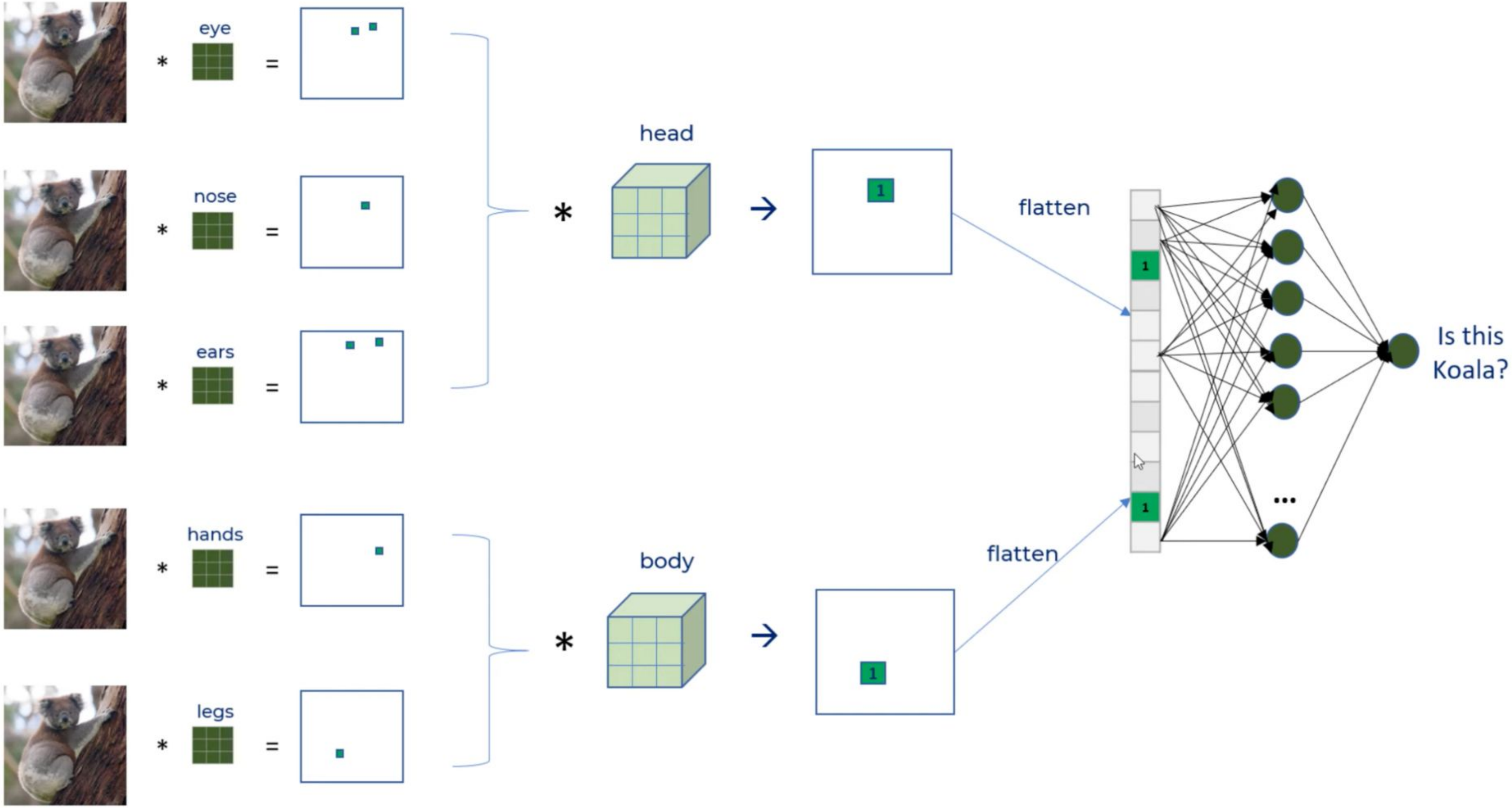


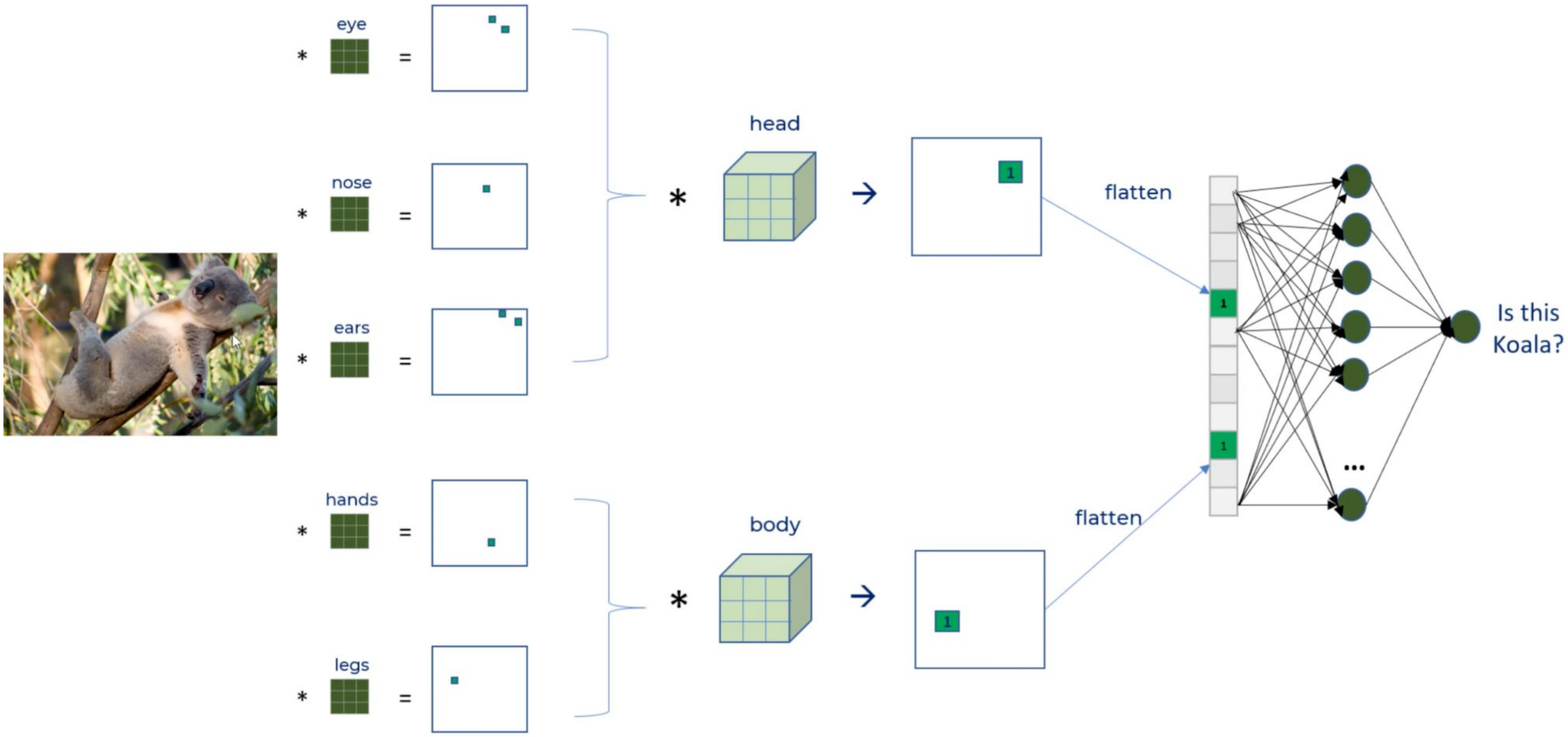


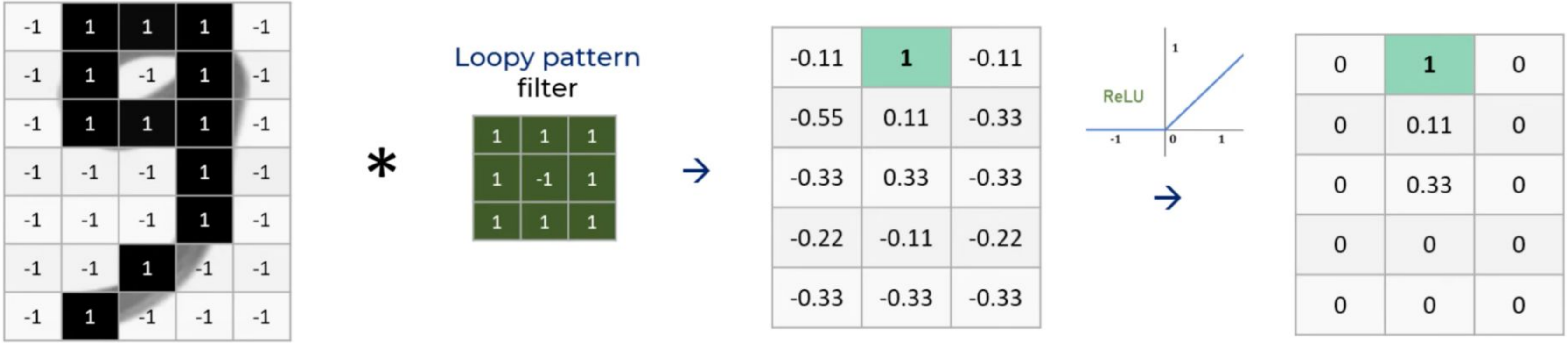
Filters

Feature Maps


eye
*
=
1
1
nose
*
=
1
ears
*
=
1
1
*
Filter for head
1


eye
nose
ears
hands
legs
*
=
head
body
1
flatten
flatten
1
1
...
Is this Koala?


eye
*
=
nose
*
=
ears
*
=
hands
*
=
legs
*
=
*
head
→
1
flatten
*
body
→
1
flatten
1
1
...
Is this Koala?



-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

*

Loopy pattern filter

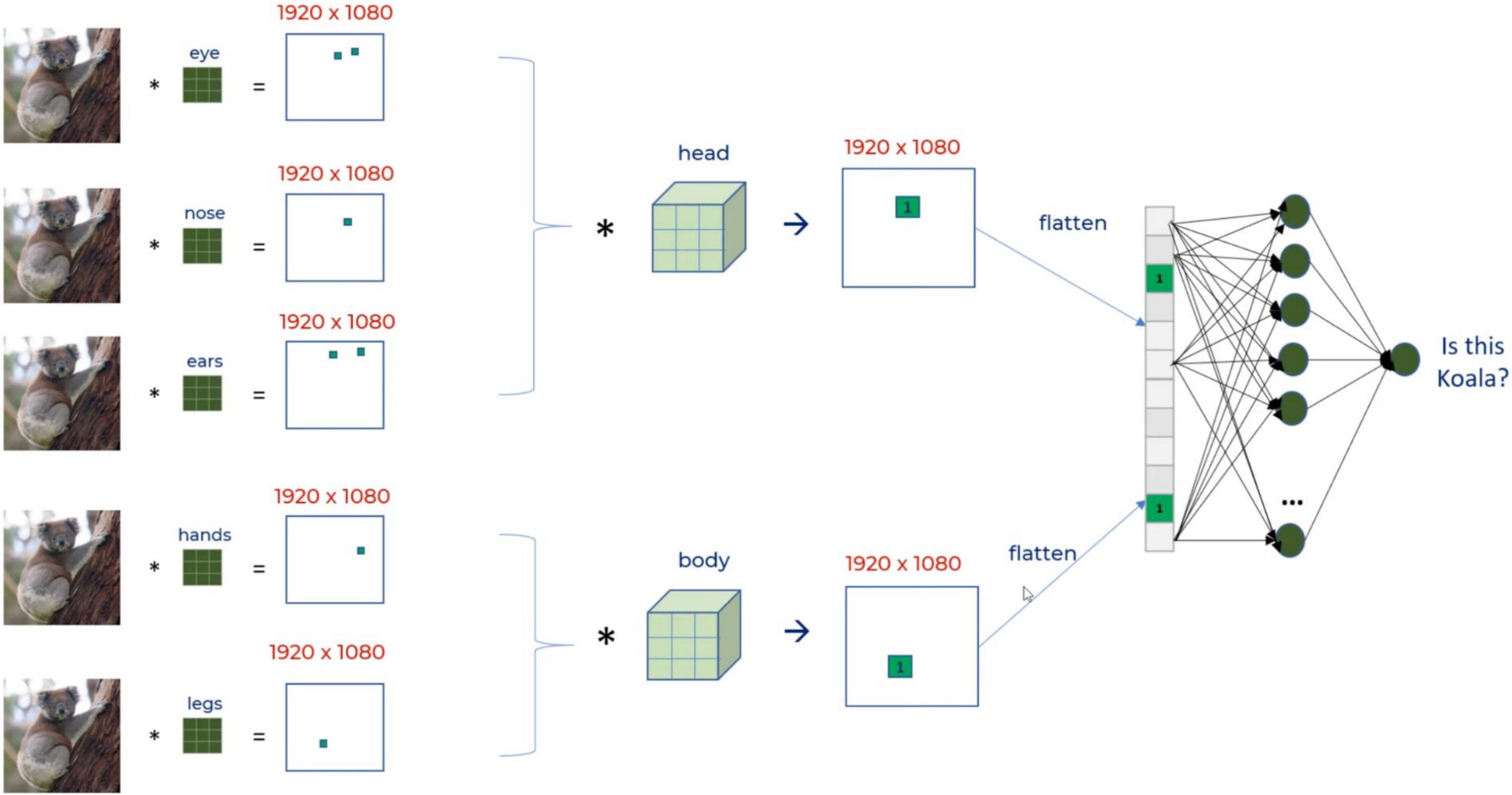
1	1	1
1	-1	1
1	1	1

→

-0.11	**1**	-0.11
-0.55	0.11	-0.33
-0.33	0.33	-0.33
-0.22	-0.11	-0.22
-0.33	-0.33	-0.33

→

0	**1**	0
0	0.11	0
0	0.33	0
0	0	0
0	0	0


1920 x 1080
eye
*
=
1920 x 1080
nose
*
=
1920 x 1080
ears
*
=
*
head
1920 x 1080
1
flatten
1920 x 1080
hands
*
=
1920 x 1080
legs
*
=
*
body
1920 x 1080
1
flatten
1
1
...
Is this
Koala?

5	1	3	4
8	2	9	2
1	3	0	1
2	2	2	0

8	**9**
3	2

2 by 2 filter with stride = 2

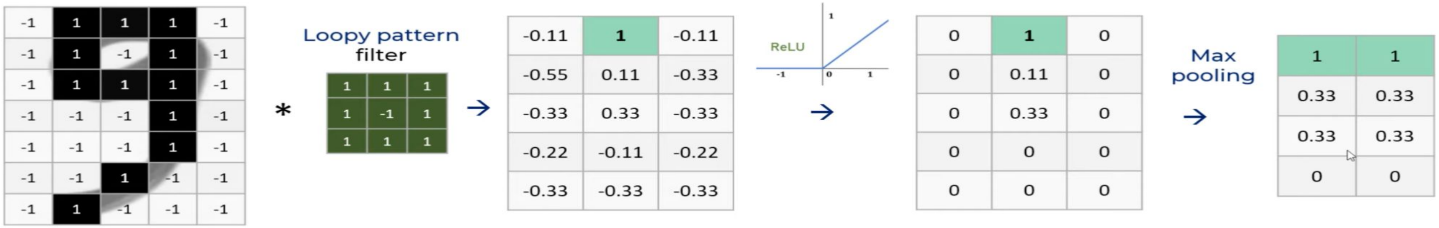
5	1	3	4
8	2	9	2
1	3	0	1
2	2	2	0

4	4.5
2	0.75

0	**1**	0
0	0.11	0
0	0.33	0
0	0	0
0	0	0

1	

2 by 2 filter with stride = 1



-1	1	1	1	-1
-1	1	-1	1	-1
-1	1	1	1	-1
-1	-1	-1	1	-1
-1	-1	-1	1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1

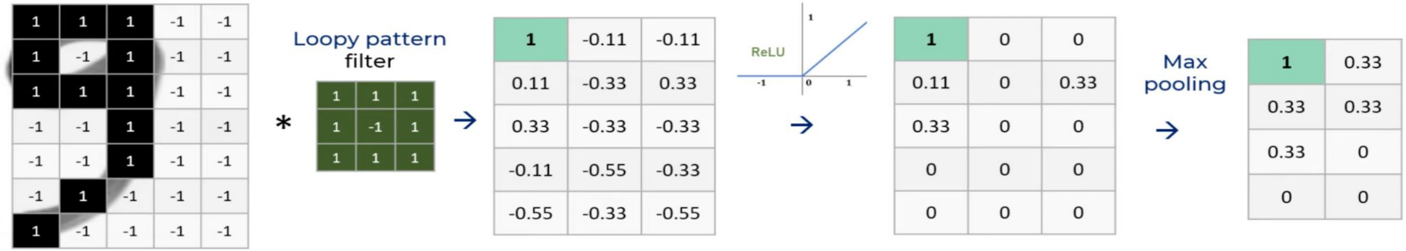
1	1	1
1	-1	1
1	1	1

-0.11	1	-0.11
-0.55	0.11	-0.33
-0.33	0.33	-0.33
-0.22	-0.11	-0.22
-0.33	-0.33	-0.33

0	1	0
0	0.11	0
0	0.33	0
0	0	0
0	0	0

1	1
0.33	0.33
0.33	0.33
0	0

Shifted 9 at different position



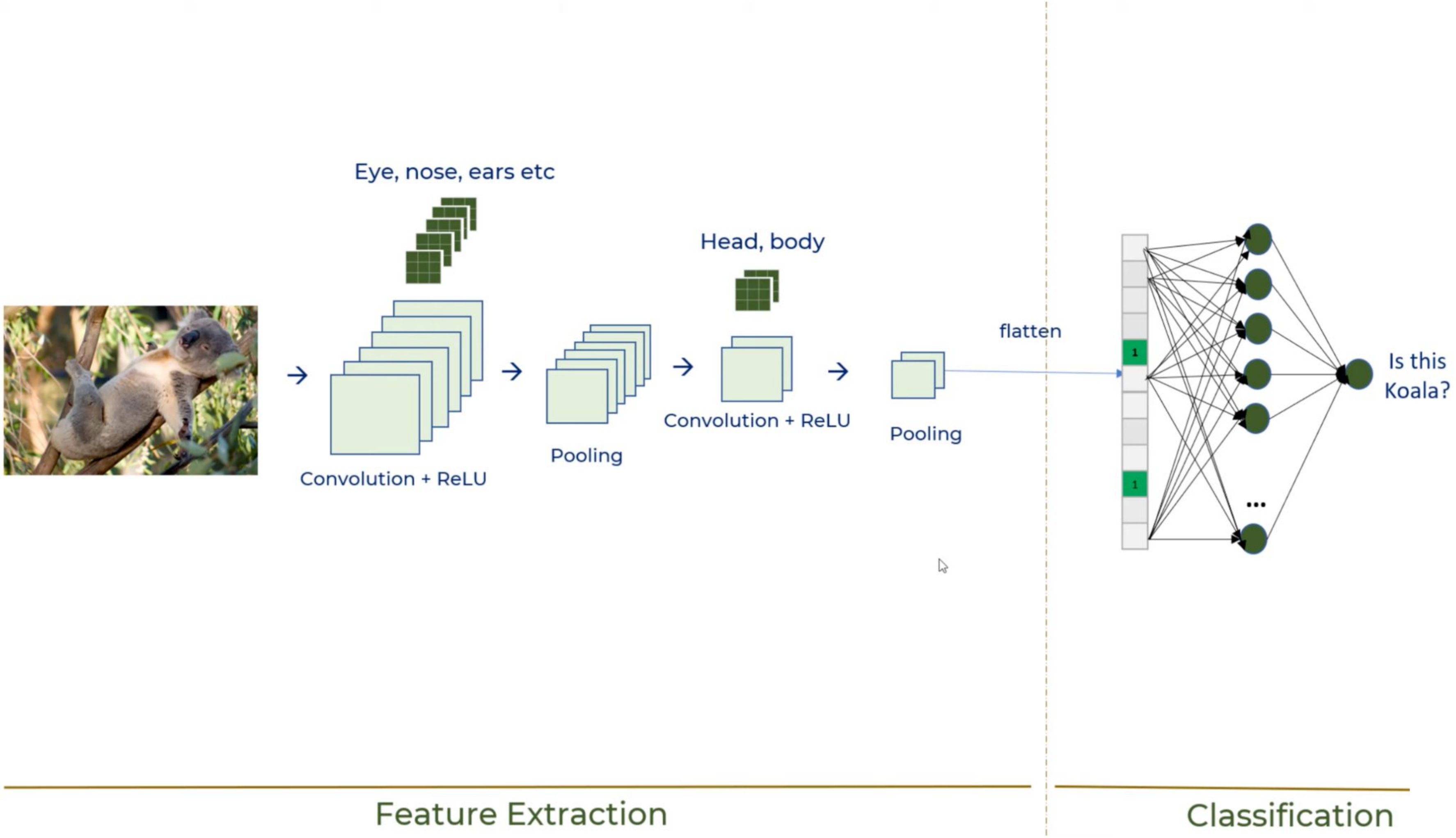
1	1	1	-1	-1
1	-1	1	-1	-1
1	1	1	-1	-1
-1	-1	1	-1	-1
-1	-1	1	-1	-1
-1	1	-1	-1	-1
1	-1	-1	-1	-1

1	1	1
1	-1	1
1	1	1

1	-0.11	-0.11
0.11	-0.33	0.33
0.33	-0.33	-0.33
-0.11	-0.55	-0.33
-0.55	-0.33	-0.55

1	0	0
0.11	0	0.33
0.33	0	0
0	0	0
0	0	0

1	0.33
0.33	0.33
0.33	0
0	0



Eye, nose, ears etc

Convolution + ReLU

Pooling

Head, body

Convolution + ReLU

Pooling

flatten

Is this Koala?

Feature Extraction

Classification