



基于机器学习的恶意代码分析

-----CNN的一次实践

为什么要做

- 分析机器码对人来说是一项极其困难和枯燥的工作，而大量的样本正适合机器学习

什么是机器学习

- 机器学习的英文名称叫**Machine Learning**，简称**ML**，该领域主要研究的是如何使计算机能够模拟人类的学习行为从而获得新的知识和技能，并且重新组织已学习到的知识和技能，使之在应用中能够不断完善自身的缺陷与不足。

什么是CNN

- 卷积神经网络（Convolutional Neural Network,**CNN**）是一种前馈神经网络，它的人工神经元可以响应一部分覆盖范围内的周围单元，对于大型图像处理有出色表现。^[2] 它包括卷积层(convolutional layer)和池化层(pooling layer)。

CNN通常是用来识别图像而不是文本的

- 通常处理这类问题我们更倾向于使用RNN,但是我们想到了一种非常有趣的方案,把汇编成机器码的代码转换成图片,然后导入到CNN里面进行训练,产生了比较理想的效果

不难看出机器码和图像在底层上是十分相似的

1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E
54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB
55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC
18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13
9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3
0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8
66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8
4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D
66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16
68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66
55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF
0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E
06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00
00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E
00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F
0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF
0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00
A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09

[210,	112,	3],
[213,	111,	12],
[200,	95,	4],
[197,	94,	0],
[212,	112,	6],
[218,	122,	8],
[214,	118,	4],
[215,	118,	4],
[221,	124,	10],
[222,	124,	10],
[214,	115,	1],
[213,	114,	1],
[215,	115,	3],
[214,	116,	2],
[213,	116,	2],
[214,	117,	4],
[210,	113,	3],
[200,	95,	4],

举一个我之前做的例子

股骨头识别

原图



1 图像分割 第一步 对半切开并把右边旋转



第二步是人工标注重点（可选）

- 毫无疑问这个操作可以明显提高准确率



画框后的图像

对于更一般的图像 我们一般会采取相反的方法

- 即让图片变得更复杂



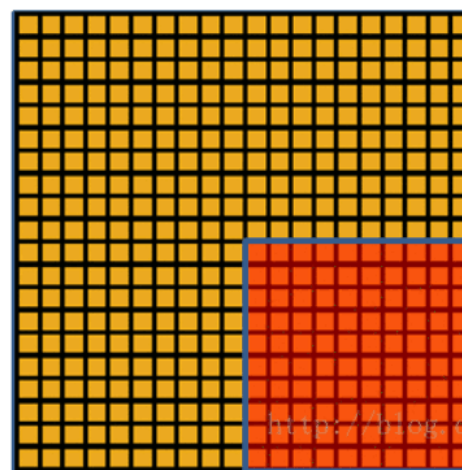
接下来就是卷积池化等一系列提取特征的方法

1	1	1	0	0
0	1	1	1	0
0	0	1 _{x1}	1 _{x0}	1 _{x1}
0	0	1 _{x0}	1 _{x1}	0 _{x0}
0	1	1 _{x1}	0 _{x0}	0 _{x1}

Image

4	3	4
2	4	3
2	3	4

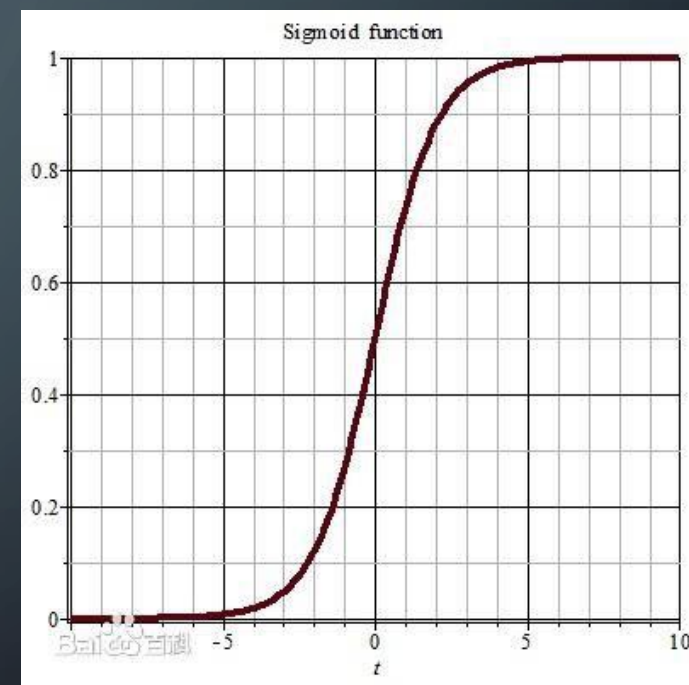
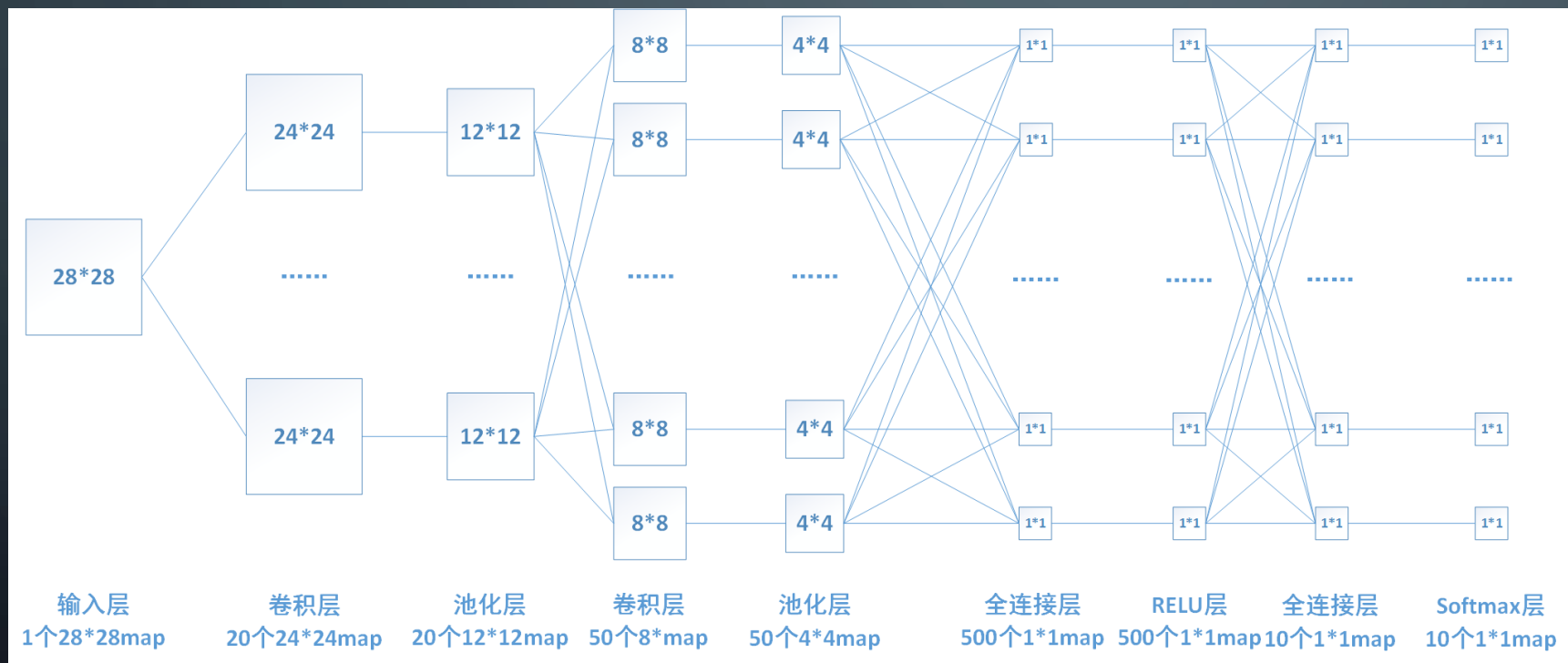
Convolved
Feature



Convolved
feature

1	7
5	9

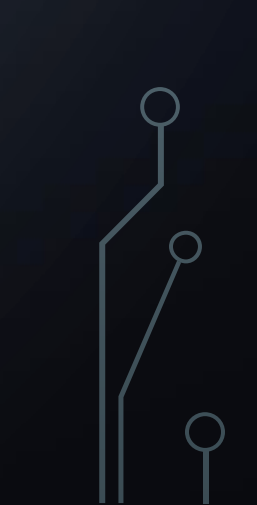

Pooled
feature





我们就使用了CNN中比较有名的框架RESNET来实现

ResNet在2015年被提出，在ImageNet比赛classification任务上获得第一名，因为它“简单与实用”并存，之后很多方法都建立在ResNet50或者ResNet101的基础上完成的，检测，分割，识别等领域都纷纷使用ResNet，Alpha zero也使用了ResNet，所以可见ResNet确实很好用。



RESNET原理

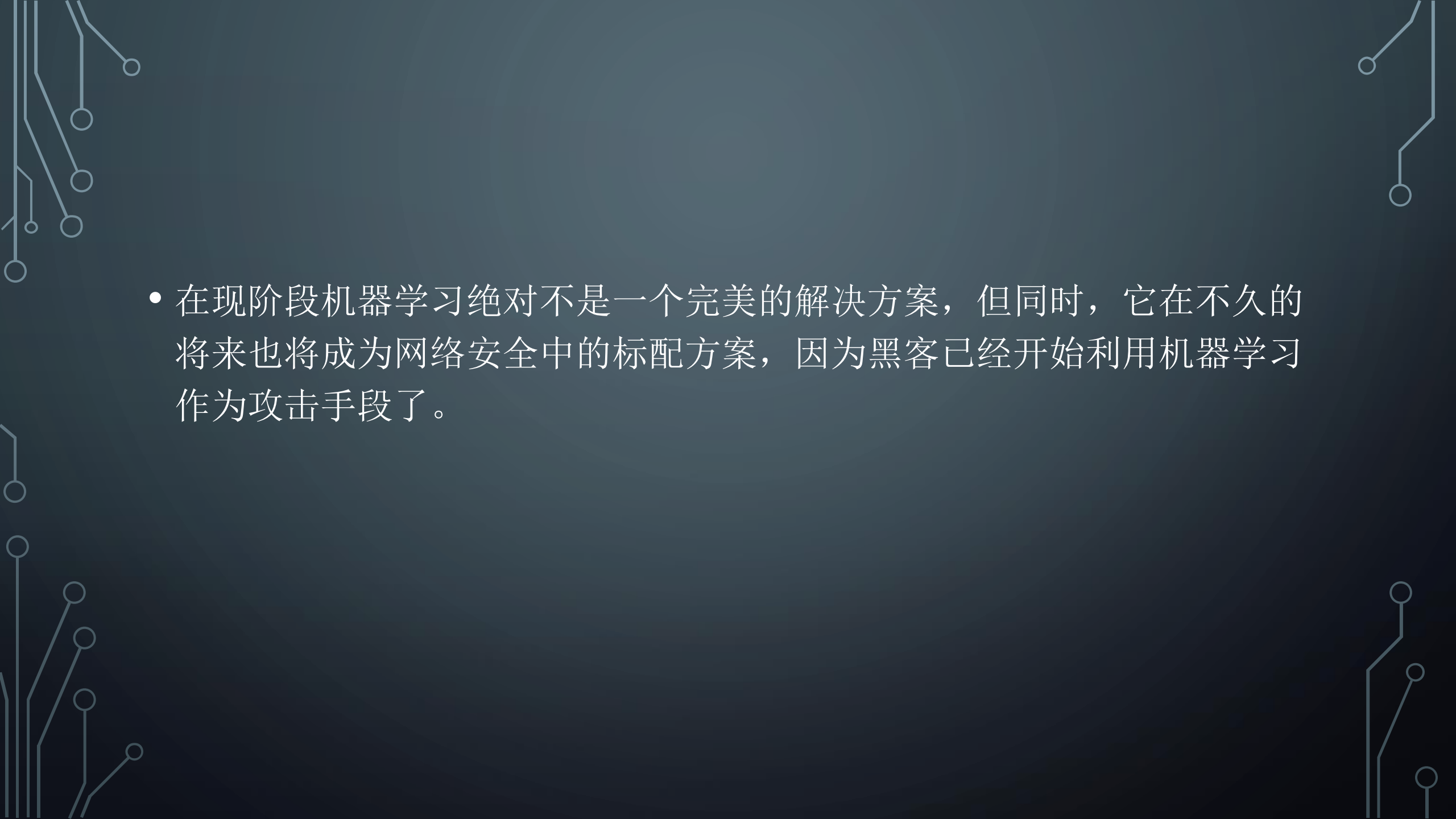
- 通常情况下我们的拟合方式是 $H(x)=x$ 的映射，而这种情况下在深度增加之后容易出现正确率反而下降的情况，所以我们把网络设计为 $H(x)=F(x)+x$ ，这样提高了相对变化率也就相应的提高了收敛速度和正确率

这种看起来很疯狂的方法奏效了

- 在我们的实验中 准确率达到了96%，很接近了人工方法的准确率了

缺点和不足

- **CNN**不适合（并不是不能）不定长输入，面对更加复杂的环境效果可能会不如**RNN**网络

- 
- The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural network connections. These elements consist of thin lines that branch out and terminate in small circles, creating a symmetrical, abstract pattern in each corner.
- 在现阶段机器学习绝对不是一个完美的解决方案，但同时，它在不久的将来也将成为网络安全中的标配方案，因为黑客已经开始利用机器学习作为攻击手段了。

The image features a dark blue background with a subtle radial gradient. In the four corners, there are decorative white line art elements resembling circuit traces or stylized branches, each ending in small circles.

谢谢大家