

# کاربرد های نوین شبکه های عصبی و یادگیری عمیق

کوروش جمشیدی  
سامان اصغری  
مجتبی ملائی  
مهتا میرزائی

دانشکده مهندسی کامپیوتر  
دانشگاه صنعتی اصفهان

۱۴۰۴ فروردین



# فهرست مطالب

۱ معرفی

۲ یک مدل CNN برای تشخیص ضربان قلب

۳ تشخیص deepfake توسط یادگیری عمیق

۴ تشخیص فیشینگ توسط CNN



# فهرست مطالب

۱ معرفی

۲ یک مدل CNN برای تشخیص ضربان قلب

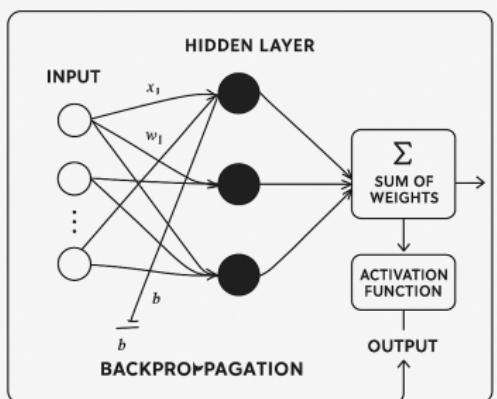
۳ تشخیص deepfake توسط یادگیری عمیق

۴ تشخیص فیشینگ توسط CNN



# شبکه عصبی

## NEURAL NETWORK

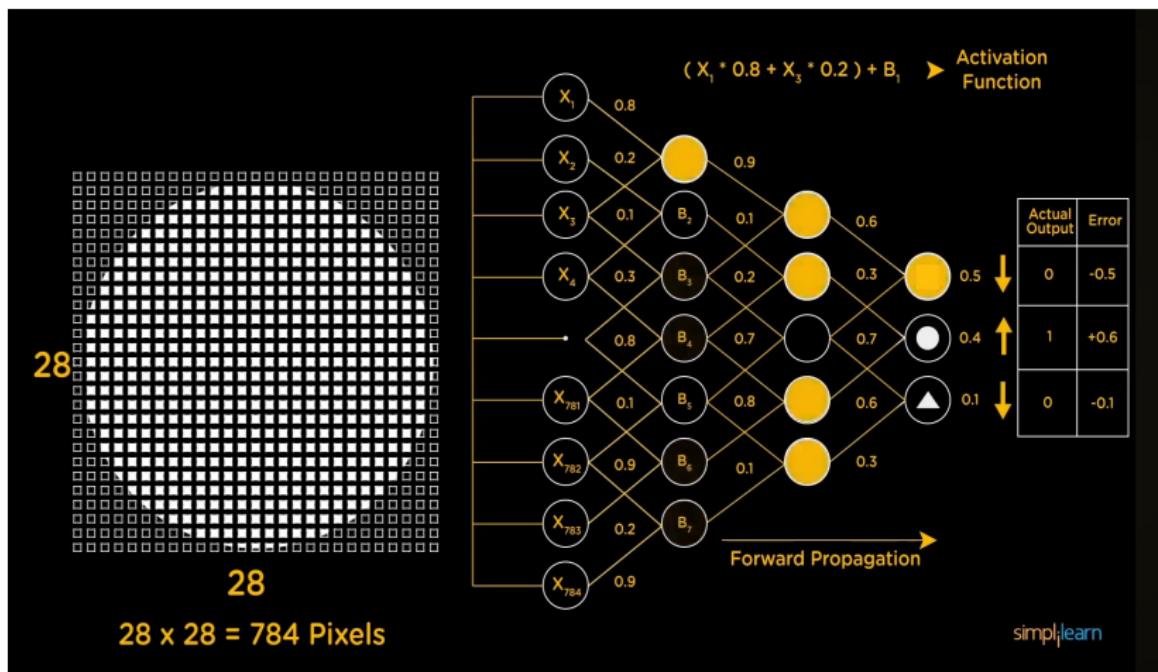


- نورون
- لایه‌های مختلف
- کانال‌ها
- Function Activation
- Propagation Forward
- تشخیص خطأ
- Propagation Backward

شکل ۱-۱: شبکه عصبی  
ساخته شده با ChatGPT



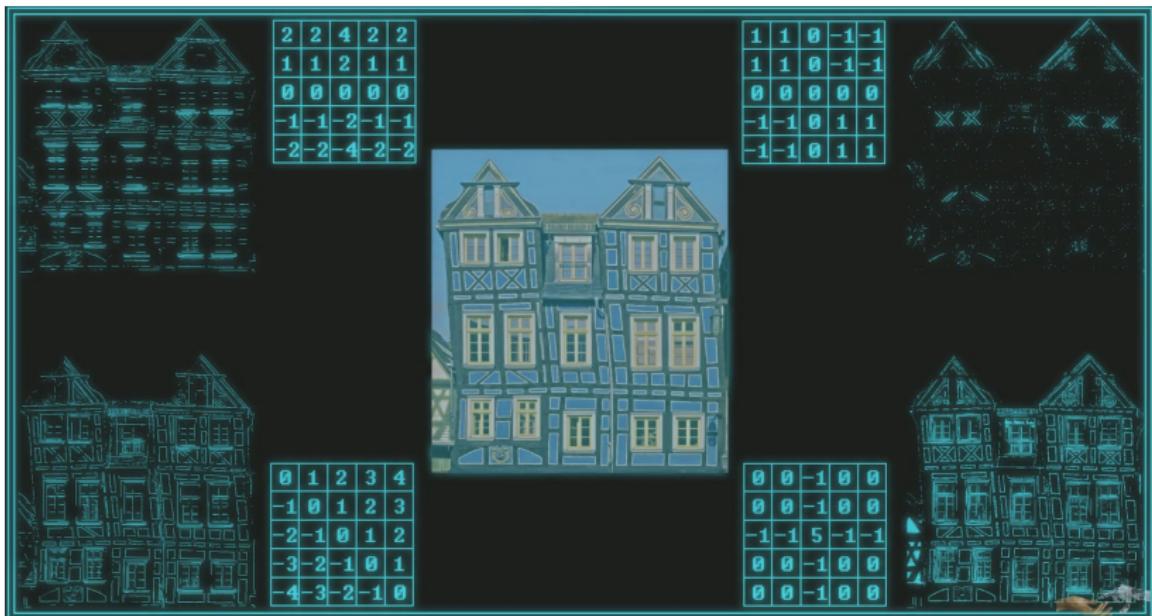
# مثال



شكل ۱-۲: یک مثال از شبکه عصبی <https://youtube.com/Simplilearn>



## شبکه های عصبی کانولوشنی (CNN)



**شکل ۱-۳:** شبکه های CNN ساخته شده با ChatGPT

# فهرست مطالب

۱ معرفی

۲ یک مدل CNN برای تشخیص ضربان قلب

۳ تشخیص deepfake توسط یادگیری عمیق

۴ تشخیص فیشینگ توسط CNN



# ECG چیست؟

- ثبت فعالیت قلب
- رسم سیگنال در قالب نمودار
- یک تست ساده و غیر قابل تهاجمی
- هر ضربان قلب نمایانگر یک سیگنال
- قابل استفاده در تشخیص بیماری



# آریتمی چیست؟

- ریتم غیرطبیعی قلب
- سریع یا کند بودن ضربان قلب
- نامنظم بودن ضربان قلب
- ECG ابزار تشخیص بیماری آریتمی



# وجود شبکه عصبی

- تفسیر دستی ECG زمانبر و دشوار
- نیاز به سیستم‌های خودکار
- افزایش دقیق و سرعت با استفاده از سیستم‌های هوشمند



# دسته بندی انواع ضربانها

- ← ضربان‌های نرمال **N**
- ← ضربان‌های فوق‌بطنی نابجا **S**
- ← ضربان‌های بطنی نابجا **V**
- ← ضربان‌های ترکیبی (فیوژن) **F**
- ← ضربان‌های ناشناخته یا غیرقابل طبقه‌بندی **Q**

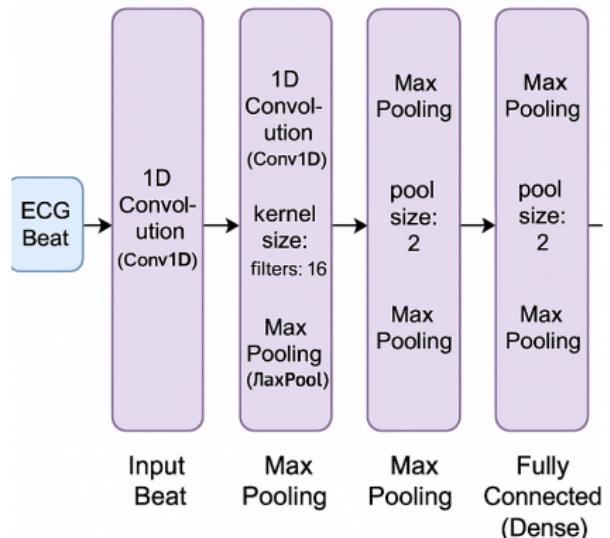


# چالش داده‌ها

- تکراری بودن دسته N
- کمبود داده‌ها در سایر دسته‌ها
- عدم دقیقیت مدل به علت ناتوازنی داده‌ها
- تولید داده مصنوعی برای تعادل
- افزایش کلاس‌های کم‌نمونه به اندازه N



# معماری شبکه

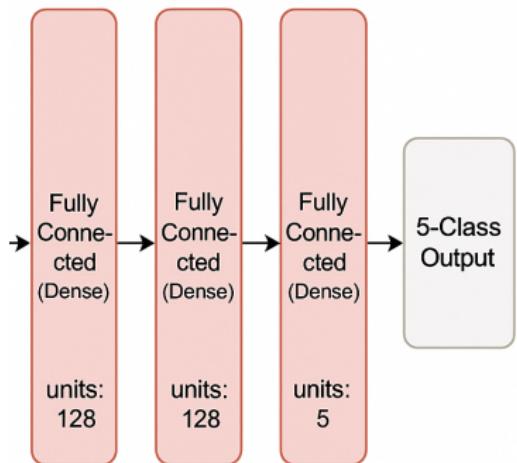


- ۳ لایه کانولوشن برای استخراج ویژگی
- ۳ لایه max pooling برای کاهش ابعاد
- فعالساز Leaky ReLU در لایه‌ها

شكل ۱-۲: قسمت اول معماری شبکه مورد نظر ساخته شده توسط ChatGPT



# معماری شبکه (ادامه)



- ۳ لایه fully connected نهایی
- خروجی softmax با ۵ دسته مختلف
- آموزش با backpropagation در ۲۰ تکرار

شكل ۲-۲: قسمت دوم معماری شبکه مورد نظر  
ساخته شده توسط ChatGPT



# نتایج

- دقیق بالا در تشخیص دسته‌ها
- عملکرد بهتر با داده تمیز (Set B)
- دقیق نهایی حدود ۹۴ درصد
- حساسیت بالا در تمام دسته‌ها
- بهترین عملکرد توسط کلاس Q



# مزایا و معایب

## مزایا

✓ کاملاً خودکار و سریع

✓ مقاوم در برابر نویز سیگنال

✓ بدون نیاز به استخراج ویژگی

## معایب

✗ آموزش سنگین و زمان بر

✗ نیاز به سخت افزار قوی

✗ احتمال وجود خطأ



# نتیجه گیری

- ✓ یک ابزار قدرتمند در پزشکی
- ✓ دقت بالا در طبقه‌بندی ضربان
- ✓ کاهش زمان بررسی ECG
- ✓ قابل اجرا در سیستم‌های بالینی
- ✓ مناسب برای غربال‌گری سریع بیماران



# فهرست مطالب

۱ معرفی

۲

۳

۴

تشخیص فیشینگ توسط CNN

۳ تشخیص deepfake توسط یادگیری عمیق

۲ یک مدل CNN برای تشخیص ضربان قلب



# Deepfake



شکل ۲-۱: ویدئو深fake جل Barack Obama  
<https://www.youtube.com/watch?v=cQ54GDm1eL0>



شکل ۲-۲: ویدئو深fake جل Nicholas Cage  
<https://www.youtube.com/watch?v=BU9YAHigNx8>

- رسانه‌ها و شبکه‌های اجتماعی
- اخبار غلط
- یادگیری عمیق
- deep learning ترکیب **deepfake**
- fake و
- تشخیص دشوار
- ایجاد محدودیت‌های جدید



# ویدئوهای از چهره افراد

## جابه جایی چهره (Face-swapping)



شکل ۳-۲: مقایسه جابه جایی چهره و بازسازی چهره  
<https://www.mdpi.com/sensors/sensors-22-04697/article-deploy/html/images/sensors-22-04697-g001-550.jpg>

- جابه جا کردن چهره فرد داخل ویدئو
- انتقال حالات صورت از فرد اصلی
- جابه جایی چهره با یک فرد مشهور
- Faceswap-GAN

## بازسازی چهره (face-reenactment)

- ثابت ماندن هویت فرد اصلی
- انتقال حالات چهره به فرد اصلی
- به حرکت در آوردن چهره در عکس
- Face2Face



# مجموعه داده‌ها (Datasets)

DataSet	Video Count
Original	1000
Deepfakes	1000
Face2Face	1000
FaceSwap	1000
NeuralTextures	1000

- FaceForensics++ •
- برای یادگیری ۸۰% •
- برای تست ۲۰% •

شکل ۲-۴: مشخصات مجموعه داده‌ها [۱]



## پیش پردازش داده ها



!  
عکس به عنوان ورودی مدل

- تبدیل ویدئو به فریم ها
- یک فریم از هر چهار فریم

!  
تشخیص بر اساس چهره

- جداسازی چهره ها
- cascade classifier

شكل ۲-۵: جدا سازی فریم و پردازش آنها [1]



## مدل های پادگیری عمیق

Xception 1

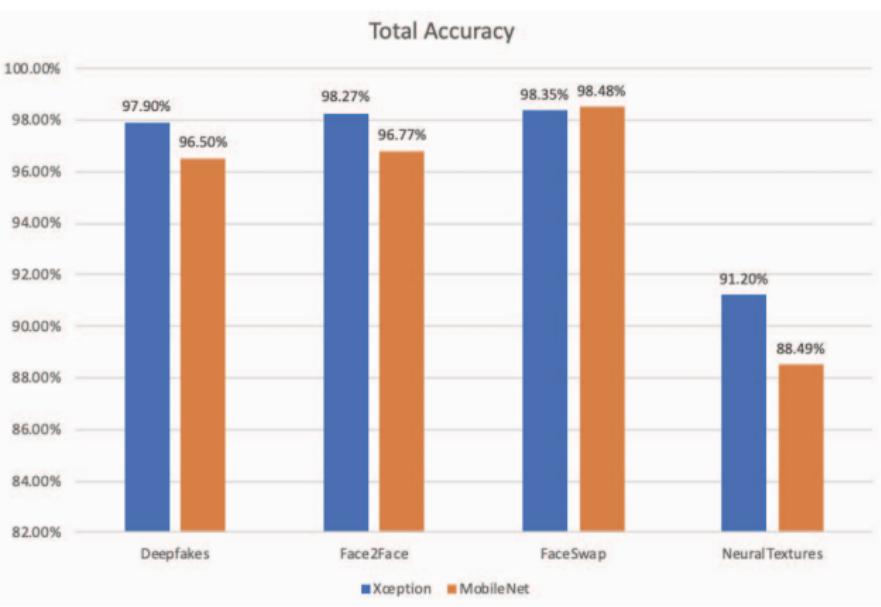
- ## CNN

MobileNets ↗

- پیاده سازی با TensorFlow
  - ۲۸ لایه سبک و بهینه
  - CNN



# نتایج



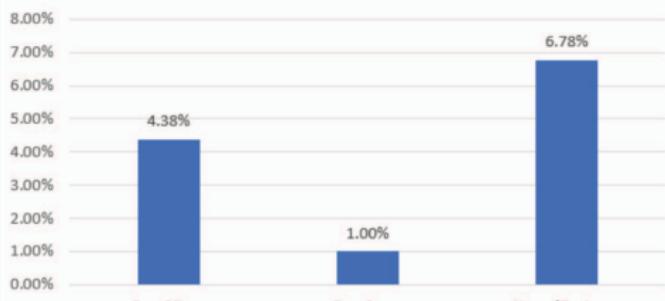
- مدل ۸
- عملکرد بهتر در Xception
- دشواری تشخیص در NeuralTexture
- تشخیص ویدئو مربوط به Obama

شكل ۶-۲: مقایسه نتایج مدل‌ها [۱]



# چالش‌ها

Deepfakes on other datasets



- ؟ چرا مدل‌های جداگانه؟
- ! ویدئوهای مربوط به مدل‌های دیگر
- ✓ مکانیزم رائیگیری

[1] Deepfakes شکل ۲-۷: بررسی مجموعه داده‌های دیگر با



# قدمی های بعدی

- تغيير تابع هزینه و Optimizer 
- بررسی جدأگانه اجزای صورت 
- تشخیص بر اساس ویدئو 



# فهرست مطالب

۱ معرفی

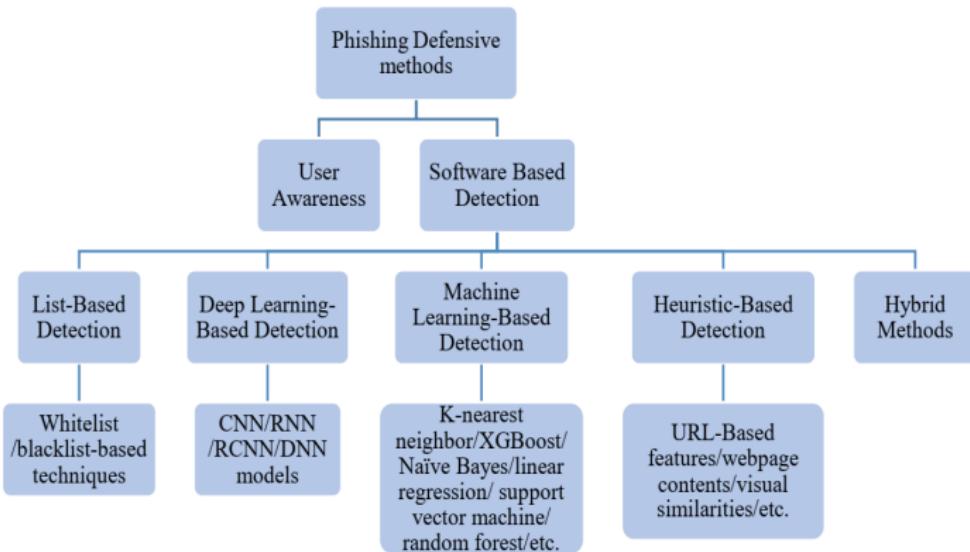
۲ یک مدل CNN برای تشخیص ضربان قلب

۳ تشخیص deepfake توسط یادگیری عمیق

۴ تشخیص فیشینگ توسط CNN



# انواع مدل‌های تشخیص فیشینگ



شكل ۱-۴: نگاهی به روش‌های تشخیص فیشینگ [۲]



# چرا تشخیص فیشینگ چالش برانگیز است؟

- شبهه ظاهری سایت های جعلی
- ناشناخته بودن حملات روز صفر
- لیست های سیاه قابل دور زدن
- نیاز به بررسی سریع و مستقل



# راهکار شبکه های عصبی: مدل CNN بر پایه URL

- ➡ ورودی فقط آدرس URL
- ➡ عدم نیاز به بررسی محتوای سایت
- ➡ مقاوم در برابر حملات روز صفر
- ➡ زمان تشخیص: ۰.۴۷ میلی ثانیه!
- ➡ مدل کاملا مستقل

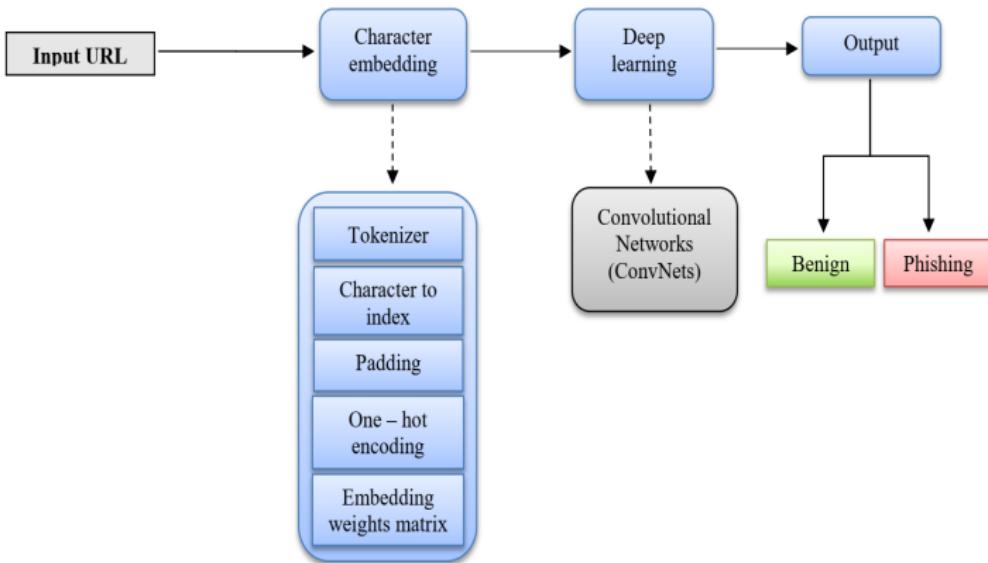


# ساختار مدل

- بردار one-hot برای هر کarakتر
- حداقل ۲۰۰ کarakتر
- ۷ لایه کانولوشن متوالی
- ۳ لایه fully connected نهایی
- خروجی: فیشینگ/عادی



# ساختار مدل (ادامه)



شکل ۲-۴: مروری بر مدل پیشنهادی [۲]



# دقت مدل

- دقت روی دیتاست مقاله: ۹۵%
- دقت روی دیتاست خارجی: ۹۸.۵۸%
- بهتر از Random Forest با دقت ۹۳.۶۲%
- سرعت و دقت در سطح بالا



# جمع بندی و کاربرد ها

- تشخیص سریع توسط URL خام
- کاربرد در مرورگر ها و فایروال ها
- مناسب برای مقابله با حملات جدید
- بدون نیاز به تخصص امنیتی
- ترکیب امنیت، یادگیری و سادگی



thank  
you!



## مراجع ا

- [1] Deng Pan et al. “Deepfake Detection through Deep Learning”. In: *2020 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)*. 2020, pp. 134–143. DOI: 10.1109/BDCAT50828.2020.00001.
- [2] Ali Aljofey et al. “An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL”. In: *Electronics* 9.9 (2020). ISSN: 2079-9292. DOI: 10.3390/electronics9091514. URL: <https://www.mdpi.com/2079-9292/9/9/1514>.
- [3] Ayush Lal, Prashant Kumar, and Suman Halder. “Heartbeat Classification Based on Deep Convolutional Neural Network”. In: *2023 International Conference on Networking and Communications (ICNWC)*. 2023, pp. 1–4. DOI: 10.1109/ICNWC57852.2023.10127341.

