

بناء وتفسير نموذج لكشف الاحتيال في المعاملات المالية باستخدام الشبكات العصبية الالتفافية (CNN)

1. مقدمة

1. تعريف المشكلة

تعتبر عمليات الاحتيال في بطاقات الائتمان من أكثر الجرائم المالية انتشاراً، حيث تكبد المؤسسات المالية والعملاء خسائر بمليارات الدولارات سنوياً. تتميز هذه العمليات بأنها سريعة ومعقدة، مما يجعل من الصعب على الأنظمة التقليدية اكتشافها. الهدف من هذا البحث هو بناء نظام آلي قادر على تحليل ملايين المعاملات وتحديد الأنماط المشبوهة بدقة عالية.

2. تحديات المشكلة

التحدي الأكبر في هذا المجال هو الطبيعة غير المتوازنة للبيانات. فعدد المعاملات الاحتيالية يمثل جزء ضئيل جداً أقل من 1% من إجمالي المعاملات. إذا تم تدريب نموذج تعلم الآلة على هذه البيانات مباشرة فإنه سيتعلم أن أسهل طريقة لتحقيق دقة عالية هي تصنيف كل شيء على أنه طبيعي وبالتالي سيفشل في تحقيق الهدف الأساسي وهو كشف الاحتيال

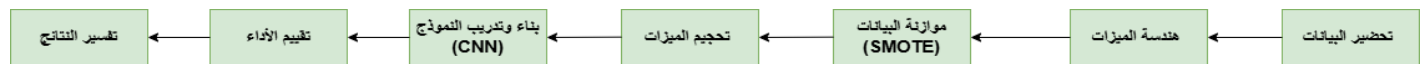
3. الهدف من البحث

يهدف هذا البحث إلى:

1. معالجة البيانات الأولية وإنشاء ميزات سياقية فعالة.
2. حل مشكلة عدم توازن البيانات باستخدام تقنيات متقدمة.
3. بناء وتدريب نموذج شبكة عصبية الالتفافية (CNN) قادر على تعلم الأنماط المعقدة.
4. تقييم أداء النموذج بشكل شامل باستخدام مقاييس مناسبة.
5. تفسير قرارات النموذج من خلال تحديد الميزات الأكثر تأثيراً.

2. منهجية العمل (Methodology)

1. نظرة عامة على سير العمل



2. الأدوات والمكتبات

تم اختيار مجموعة من المكتبات الرائدة في مجال علم البيانات وتعلم الآلة:

- **Pandas & NumPy**: هما العمود الفقري لمعالجة البيانات في python. تم اختيارهما لسرعهما ومرونتهما في التعامل مع جداول البيانات الكبيرة والعمليات الحسابية المعقدة.
- **Scikit-learn**: هي المكتبة القياسية لمهام تعلم الآلة التقليدية تم استخدامها لتقسيم البيانات (train_test_split)، وتجسيم الميزات (StandardScaler)، وحساب مقاييس الأداء الدقيقة (classification_report، confusion_matrix، roc_auc_score).
- **Imbalanced-learn (SMOTE)**: تم اختيار هذه المكتبة خصيصاً لتقديم حل متقدم لمشكلة عدم توازن البيانات. تقنية SMOTE تتفوق على الحلول البسيطة مثل التكرار العشوائي حيث تقوم بإنشاء عينات جديدة وذات معنى.
- **TensorFlow & Keras**: تم اختيار Keras كواجهة برمجية عالية المستوى لـ TensorFlow لبناء الشبكات

العصبية. يتميز keras بسهولة الاستخدام وسرعة بناء النماذج المعقدة مثل cnn مع توفير المرونة الكاملة لتخصيص كل طبقة.

- **Matplotlib & Seaborn:** تم استخدامهما لإنشاء رسوم بيانية واضحة واحترافية أمر ضروري لتصوير أداء النموذج وتفسير النتائج

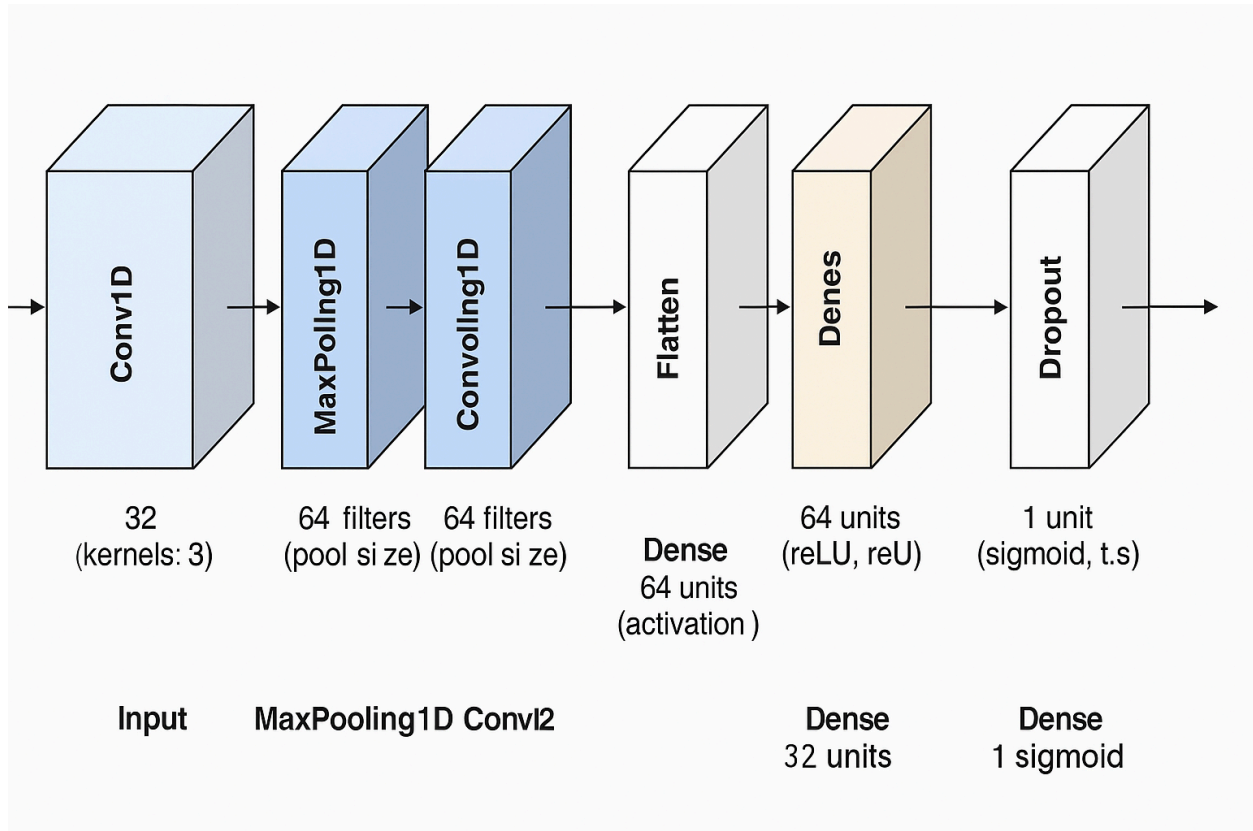
3. المعالجة المسبقة وهندسة الميزات

تم تطبيق دالة preprocess_data على البيانات لإنشاء ميزات سياقية مهمة، مثل استخراج الساعة واليوم والشهر من عمود الوقت، وترميز المتغيرات الفئوية (النصية) مثل category و gender إلى أعمدة رقمية

4. تقنية موازنة البيانات (SMOTE)

لمعالجة مشكلة عدم توازن البيانات تم استخدام تقنية smote على بيانات التدريب فقط تقوم هذه التقنية بإنشاء عينات احتيالية اصطناعية جديدة بناء على خصائص العينات الحقيقية المجاورة لها هذا يؤدي إلى مجموعة بيانات تدريب متوازنة مما يجبر النموذج على تعلم الأنماط الاحتمالية بفعالية

5. تصميم النموذج (CNN)



تم اختيار بنية الشبكة العصبية الالتفافية cnn لأنها قادرة على اكتشاف الأنماط المحلية في تسلسل الميزات تتكون البنية من :
المدخلات (Input):

- هذه الطبقة الأولى التي تستقبل بيانات المعاملة بعد معالجتها وتحويلها إلى أرقام كل معاملة تدخل كمتجه من الميزات (features).

Conv1D (الطبقة الالتفافية الأولى):

- **32 (kernels: 3):** هذه الطبقة تعمل كعين النموذج. تحتوي على 32 مرشح فلتير كل مرشح بحجم 3 يقوم بالمرور على بيانات الإدخال للبحث عن أنماط محلية صغيرة على سبيل المثال، علاقة بين 3 ميزات متجاورة.

MaxPooling1D (طبقة التجميع):

- بعد اكتشاف الأنماط تقوم هذه الطبقة بتقليل حجم البيانات عن طريق أخذ القيمة القصوى من كل مجموعة صغيرة هذا يساعد على الحفاظ على أهم الميزات المكتشفة ويجعل النموذج أسرع

Conv1D (الطبقة الالتفافية الثانية والثالثة):

- **64 filters:** هاتان الطبقتان تقومان بنفس وظيفة الطبقة الأولى ولكن بعدد أكبر من المرشحات 64 هذا يسمح للنموذج بتعلم أنماط أكثر تعقيد وتجريد بناء على الأنماط البسيطة التي تم اكتشافها في الطبقة الأولى

Flatten (طبقة التسوية):

- تقوم هذه الطبقة بتحويل البيانات متعددة الأبعاد الناتجة عن الطبقات الالتفافية إلى متجه واحد 1D لتجهيزها للطبقات العصبية العادية

Dense (الطبقات الكثيفة المتصلة بالكامل):

- **Dense 64 units, activation:** هذه هي الطبقة العصبية الأولى التي تعمل كعقل النموذج تحتوي على 64 خلية عصبية وتستخدم دالة التنشيط ReLU لاتخاذ قرارات بناء على الأنماط المستخرجة
- **Dense 32 units:** طبقة أخرى لزيادة تعقيد النموذج وقدرته على التعلم

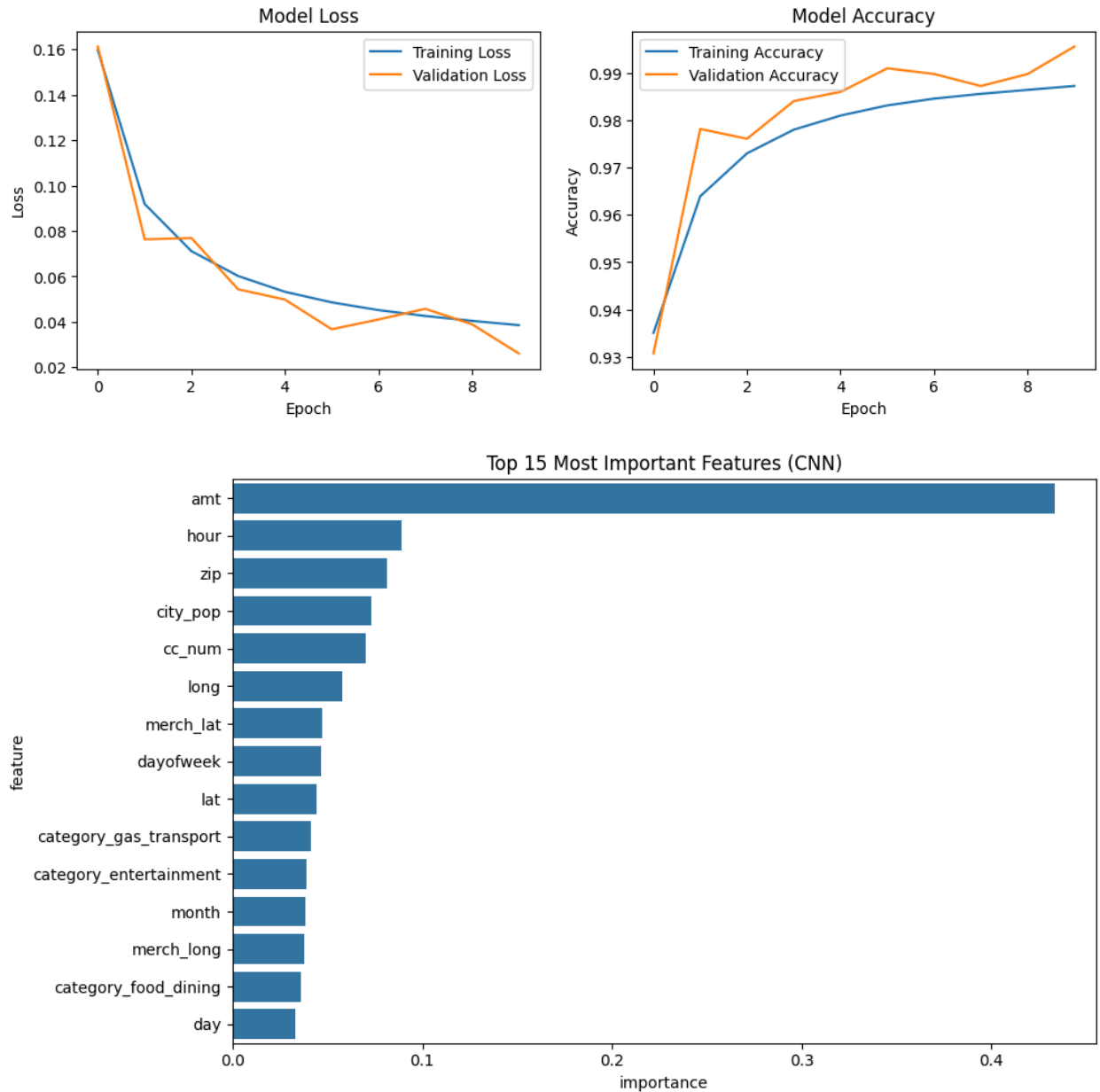
Dropout (طبقة الإسقاط):

- هذه طبقة مهمة لمنع الحفظ الزائد Over Fitting تقوم بإطفاء بعض الخلايا العصبية بشكل عشوائي أثناء التدريب مما يجبر النموذج على أن يكون أكثر قوة

Dense 1 unit, sigmoid

- هذه هي الطبقة النهائية تحتوي على خلية عصبية واحدة وتستخدم دالة التنشيط **sigmoid** لإخراج النتيجة وهي عبارة عن رقم بين 0 و 1 يمثل احتمالية أن تكون المعاملة احتيالية

3. النتائج والتحليل



1. منحنيات التدريب

تظهر الرسوم البيانية التالية أداء النموذج أثناء عملية التدريب على مدى 10 دورات epochs

- **منحنى الخسارة (Model Loss):** نلاحظ انخفاض مستمر في كل من خسارة التدريب وخسارة التحقق مما يشير إلى أن النموذج يتعلم بشكل فعال
- **منحنى الدقة (Model Accuracy):** نلاحظ ارتفاع مستمر في دقة التدريب والتحقق، وتقاربهما من بعضهما البعض يدل على أن النموذج لم يعاني من مشكلة الحفظ الزائد بشكل كبير

2. مقاييس الأداء

Classification Report:

	precision	recall	f1-score	support
0	1.00	0.99	0.99	368549
1	0.26	0.90	0.40	1930
accuracy			0.99	370479
macro avg	0.63	0.94	0.70	370479
weighted avg	1.00	0.99	0.99	370479

Confusion Matrix:

```
[[363568 4981]
 [ 187 1743]]
```

AUC-ROC: 0.9918

Average Precision: 0.8061

- **تقرير التصنيف:**
 - **Recall (1): 90%** - نتيجة ممتازة وتعني أن النموذج نجح في تحديد 90% من جميع حالات الاحتيال الفعلية.
 - **Precision (1): 26%** - نتيجة منخفضة وتعني أن هناك عدد كبير من الإنذارات الكاذبة.
- **مصفوفة الارتباك:**
 - **[[1743 ,187] , [4981 ,363568]]:**
 - **1743 (True Positives):** عدد حالات الاحتيال التي تم كشفها بشكل صحيح
 - **187 (False Negatives):** عدد حالات الاحتيال التي فشل النموذج في كشفها وهو رقم منخفض جداً.
 - **4981 (False Positives):** عدد المعاملات الطبيعية التي تم تصنيفها خطأً كاحتيال الإنذارات الكاذبة.
- **AUC-ROC 0.9918:** درجة قريبة جداً من 1 مما يدل على قدرة ممتازة للنموذج على التمييز بين الفئتين بشكل عام

3. أهمية الميزات

الرسم البياني التالي يوضح أهم 15 ميزة اعتمد عليها النموذج

- **amt (المبلغ):** كما هو متوقع هو العامل الأكثر أهمية بفارق كبير
- **hour (الساعة):** ثاني أهم عامل مما يؤكد أن وقت المعاملة حاسم في تحديد الاحتيال
- **الميزات الجغرافية:** zip, city_pop, long, lat تلعب دور مهم مما يشير إلى وجود أنماط جغرافية للاحتيال