Aplicando modelo de aprendizagem supervisionada para apoio ao score de autenticação biométrica

Larissa Mukuno[1], Erick Takeshi Moraes[1], Rafael Mansur Haddad[1], Eduardo C. Almeida[2]
unico[1]
Praça Gen. Gentil Falcão, 108 - Brooklin Novo, São Paulo - SP
{larissa.mukuno,erick.moraes,rafael.haddad}@unico.io
UFPR[2]
Curitiba - PR
eduardo@inf.ufpr.br

Abstract. *Facial recognition is already a part of our lives. Most smartphones can be unlocked using the face, as a way to identify the owner and provide access to data. However, it has also been gaining ground for other goals, especially in corporate solutions such as access control, document validation and online shopping. In order to increase the accuracy of our biometric score, a risk calculation model was developed that takes into account consumer behavior, based on their transaction history, aiming at reducing fraud.*

Resumo. *O reconhecimento facial já faz parte na vida de muitos de nós. Grande parte dos smartphones atuais efetua o desbloqueio do aparelho utilizando a face como forma de identificar o dono do aparelho e proporcionar acesso aos dados. No entanto, ele também vem ganhando espaço para outros objetivos, principalmente em soluções corporativas como controle de acessos, validação de documentos e para compras online. A fim de aumentarmos a acurácia de nosso score biométrico, foi desenvolvido um modelo de cálculo de risco que leva em consideração o comportamento do consumidor, baseado em seu histórico de transações, visando a diminuição de fraudes.*

1.INTRODUÇÃO

A unico é a primeira IDTech brasileira a oferecer soluções de biometria facial e admissão digital incluindo em seu portfólio de clientes as principais empresas financeiras, bancos e grandes empresas varejistas do Brasil[1]. Uma das soluções disponíveis é o *unico*|*check* que fornece uma pontuação de risco de clientes pessoa física também chamado *score* de autenticação. Esta solução é integrada ao sistema de biometria da unico no processo chamado de autenticação da pessoa física com o objetivo de validar as fotos coletadas com os CPFs fornecidos no momento do cadastro. O *score de autenticação* representa a probabilidade de uma pessoa física que está tirando uma foto ser a verdadeira titular do número de CPF fornecido. A autenticação da pessoa física pode ser positiva ou negativa dependendo do *score de autenticação* atribuído pela solução. O cálculo do *score de*

[1] https://unico.io/quem-somos/

autenticação é feito sobre a maior base biométrica facial do Brasil reunida pela unico com processamento de mais de 10 milhões de faces por mês.

O reconhecimento facial já faz parte da vida de muitos de nós. Grande parte dos *smartphones* atuais efetua o desbloqueio do aparelho com a imagem do rosto, como forma de identificar o dono do aparelho e proporcionar acesso aos dados. No entanto, o reconhecimento facial também vem ganhando espaço para outros objetivos, principalmente em soluções corporativas. Um sistema de reconhecimento facial nada mais é que software que mapeia as características faciais de uma pessoa [Zanlorensi et al., 2021]. São identificados cerca de 80 pontos nodais de uma face - como largura do nariz, distância e profundidade entre os olhos - e a ferramenta tem a capacidade de detectar e coletar essas características, gerando uma "identidade facial" e transformando-a em código numérico. Em um banco de dados previamente definido, por meio da utilização de algoritmos que comparam a imagem real com a imagem armazenada, essa identidade é confrontada com imagens presentes no sistema. Assim, a solução poderá determinar o nível de similaridade entre o rosto avaliado e a imagem já presente no banco (*score* biométrico). Uma das principais vantagens do sistema de reconhecimento facial é a prevenção de fraude nas transações - principalmente financeiras - onde um golpista pode utilizar documentos roubados para efetuar golpes. Nossa solução vem sendo utilizada por empresas de vários setores, como bancos, adquirentes, marketplaces e varejistas.

Neste artigo curto nos restringimos à autenticação negativa, ou seja, a detecção de casos suspeitos que são pessoas físicas que desejam se cadastrar nos sistemas de nossos clientes trapaceando de alguma forma o sistema de biometria. Devido à rápida mudança de comportamentos suspeitos, faz-se necessário a atualização periódica dos processos de validação de biometria e outros métodos para mitigar a autenticação de fraudadores.

A fim de aumentarmos a acurácia de nosso *score* biométrico, foi desenvolvido um modelo para calcular o *score* de risco*,* que leva em consideração o comportamento do consumidor, baseado em seu histórico de transações, visando a diminuição de fraudes.

Este estudo está divido em Metodologia, referente aos métodos de escolha do período, seleção de variáveis, escolha e aplicação do modelo; resultados preliminares e discussão, onde mostramos os principais avanços com a aplicação do algoritmo; e as considerações finais, onde indicamos os próximos passos para uma possível melhora nos indicadores de acurácia.

2. METODOLOGIA

Para melhor entendimento, dividimos a metodologia nas seguintes etapas: fluxo da biometria; criação de variáveis; escolha da safra e amostragem; análise descritiva e seleção das variáveis; treinamento do algoritmo; aplicação do modelo em outra safra.

2.1 Fluxo da biometria

De maneira sucinta, o fluxo começa quando o cliente nos envia uma imagem capturada por uma foto e um número do documento. Nosso motor biométrico faz uma série de verificações, como por exemplo, se a pessoa tirou foto de uma outra foto, se a foto é ao vivo, se o rosto é de um humano, entre outros. O próximo passo é a comparação da foto

enviada, com a imagem que temos em nosso banco de dados. Um algoritmo calcula a similaridade entre as faces e retorna um valor de *score* biométrico para o cliente. A esteira é apresentada na Figura 1.

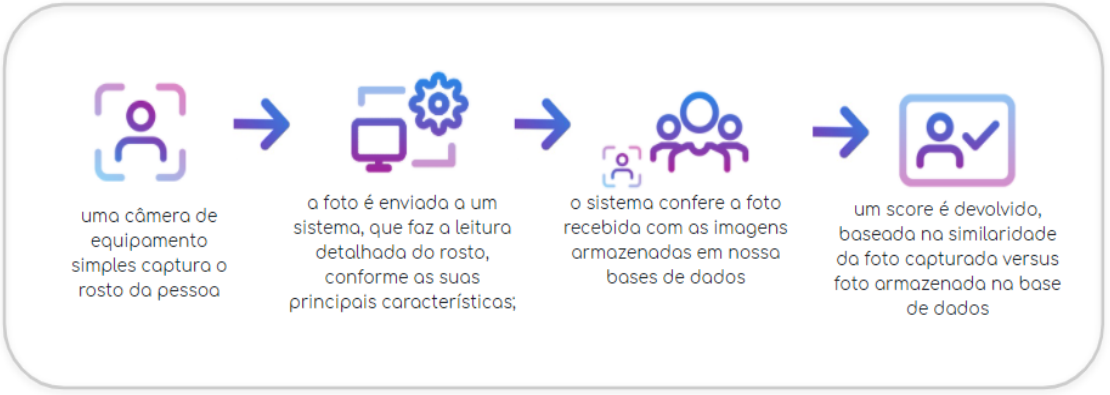

Figura 1. Fluxo da biometria

2.2 Criação de variáveis

Um dos principais desafios encontrados foi a construção de um dicionário de variáveis, devido às poucas informações referentes à pessoa que está realizando a transação. Essencialmente, recebemos o número do documento e a foto para validação biométrica. A Figura 2 apresenta as etapas para geração do modelo para calcular o *score* de risco iniciando pela etapa de extração de dados para a criação de variáveis.

Com base nas informações existentes no *Data Warehouse* (*DW*)[2] relativas à transação e estudos internos relacionados à fraude, foi criado um book de informações (dataset com variáveis sumarizadas, correspondentes às transações) contendo dezenas de indicadores.

2.3 Escolha da safra e amostragem

Para a amostragem, foram escolhidas transações dos últimos 2 anos. O motivo da escolha de um período longo foi para termos uma quantidade significativa de registros fraudulentos, a fim de que o modelo consiga classificar o que é fraude e não fraude.

Devido à característica de nossa carteira, com número baixo de fraudes em relação à quantidade total de transações (abaixo de 1%), escolhemos a técnica de oversampling, onde aumentamos o percentual de fraudes detectadas, resultando em um *dataset* com a proporção de 50% de casos de fraude e 50% de casos de não fraude.

2.4 Análise descritiva e seleção das variáveis

Para tratamento dos dados, foi utilizada a análise descritiva, a fim de detectarmos anomalias, como valores excessivamente altos ou muito baixos (*outliers*), variáveis com informações faltantes (*missings*) e retirá-las do estudo.

---

[2] "Um data warehouse é um tipo de sistema de gerenciamento de dados projetado para ativar e fornecer suporte às atividades de business intelligence (BI), especialmente a análise avançada. [...] geralmente contêm grandes quantidades de dados históricos. Os dados em um data warehouse geralmente são derivados de uma ampla variedade de fontes, como arquivos de log de aplicativos e aplicativos de transações." https://www.oracle.com/br/database/what-is-a-data-warehouse/

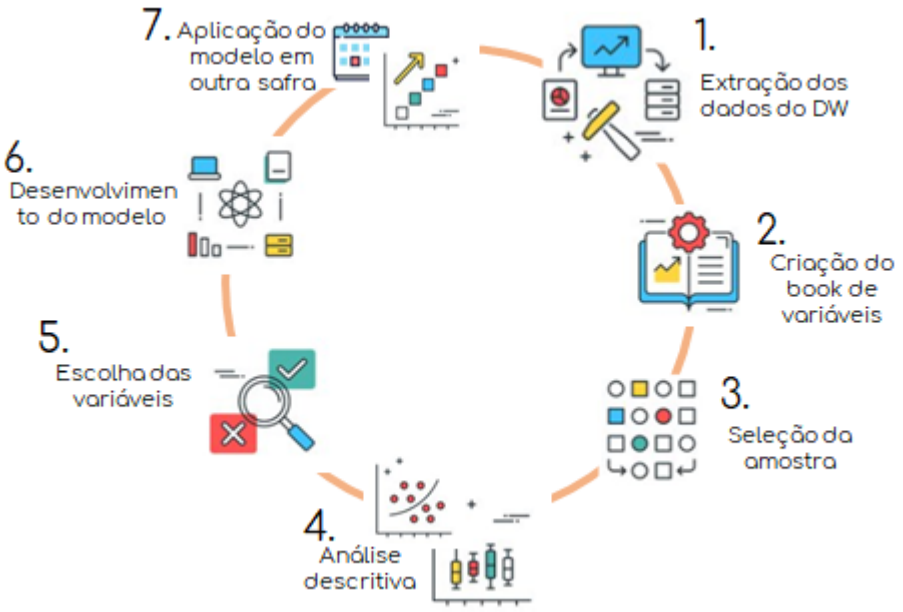

Figura 2. Etapas para geração do modelo

O passo seguinte foi a escolha dos melhores indicadores por meio do IV (*Information Value*), que indica quanto uma variável é boa para explicação da variável resposta (no caso do estudo, um fraudador de um não fraudador) [Beraldi, 2014]. Consideramos índices entre 0,1 e 0,5 como ponto de corte para manter no estudo [Siddiqi, 2006]. Finalmente, retiramos variáveis com alta correlação entre si, e análise do VIF (*Variance Inflation Factor*), que verifica a multicolinearidade, evitando a inclusão de variáveis não significativas e que não farão diferença se adicionadas no modelo. Desconsideramos indicadores com VIF > 10 (Hair et al. 1995). Dentre as dezenas de variáveis, 40 foram escolhidas para serem testadas no modelo.

2.5 Treinamento do algoritmo

Foi escolhido o algoritmo de regressão logística [Beraldi, 2014] pelos três principais motivos: facilidade de interpretação dos coeficientes por pessoas menos técnicas; fácil implantação no ambiente de produção; output simples e de fácil entendimento. Outros algoritmos foram testados, porém a regressão logística foi o que apresentou melhor resultado. Após a validação dos pesos dos coeficientes, o modelo selecionou 11 variáveis preditoras. O resultado é um *score de risco* entre 0 e 1000, onde o maior valor indica menor probabilidade de fraude.

2.6 Aplicação do modelo em safra de dados diferente

Para evitar possível overfitting, o modelo foi aplicado à dados de outra safra de dados, também chamada de *out-of-time*. A utilização dessa base se mostra importante para verificar quão preciso é o modelo ao prever indivíduos que não estão na base de desenvolvimento. Constatamos que o modelo manteve o poder preditivo semelhante à safra de dados de desenvolvimento.

3. RESULTADOS PRELIMINARES

A partir do resultado obtido pelo modelo, foram criados vários cenários, levando em conta o equilíbrio entre uma maior autenticação (e consequente aumento no número de fraudes) e menor autenticação (com menos casos de fraude). Mantendo-se o mesmo patamar de fraudes detectadas, aumentamos em 4,43% a quantidade de autenticações (+- 100 mil transações a mais no período). Em um cenário visando-se uma maior autenticação, conseguimos aumentar em 14% a quantidade de autenticações, com aumento de 0,003% na taxa de erro.

Após a implantação do modelo em ambiente de produção, acompanhamos periodicamente os valores de adesão para cada um dos clientes, assim como a quantidade de fraudes detectadas, por meio de um relatório de monitoramento. A partir dos resultados, verificamos que uma divisão por segmento melhoraria os resultados de adesão e diminuição da taxa de erro, criando regras específicas de acordo com o perfil do cliente. O monitoramento também nos mostrou uma mudança brusca no perfil de alguns clientes, provavelmente um reflexo da pandemia do coronavírus, dado que em algumas regiões do Brasil o comércio permaneceu fechado durante um período (migração dos clientes que transacionavam presencialmente e mudaram para o meio digital), fazendo-se necessária a alteração de algumas regras em determinados cenários.

4. CONCLUSÃO E CONSIDERAÇÕES FINAIS

Este artigo curto brevemente apresenta a solução *unico| check* para prevenção de fraudes em transações *online*. A solução é desenvolvida pela unico, a primeira IDTech brasileira a oferecer soluções de biometria facial e admissão digital. Este estudo mostra que temos um ganho considerável quando levamos em conta a utilização de dados históricos de transação para auxiliar na autenticação biométrica. Há muitas oportunidades para melhorar o desempenho do modelo de *score* de autenticação. Dentre as oportunidades que a unico está explorando em parceria com pesquisadores da Universidade Federal do Paraná (UFPR), estão: a segmentação de setores de empresas com o mesmo tipo de comportamento da transação, a utilização de algoritmos não supervisionados de Aprendizado de Máquina (*Machine Learning*) para identificação de outliers e um sistema de monitoramento para avaliação online. Nosso trabalho futuro se concentra na verificação de mudança de perfil de fraude e na utilização de mais informações cadastrais referente ao documento da transação.

Referências

Beraldi, F. Atualização dinâmica de modelo de regressão logística binária para detecção de fraudes em transações eletrônicas com cartão de crédito. Dissertação de Mestrado, USP, 2014.

Hair, J. F. Jr., Anderson, R. E., Tatham, R. L. & Black, W. C. (1995). Multivariate Data Analysis (3rd ed). New York: Macmillan.

Siddiqi, Naeem (2006). Credit Risk Scorecards: Developing and Implementing Intelligent Credit Scoring. SAS Institute, pp 79-83.

Zanlorensi, L., Rayson Laroca, Eduardo Luz, Alceu S. Britto Jr., Luiz S. Oliveira, David Menotti. Ocular Recognition Databases and Competitions: A Survey (2011). Wireless Sensor Networks to Control Radiation Levels. https://arxiv.org/abs/1911.09646, 2021.