Identificação de teclas a partir da vibração resultante do pressionamento

Aguinaldo Cardozo da Costa Filho, João Sinohara Silva Sousa
Renam Silva, Rodrigo Lantyer Marques Dantas

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP)
Campus São José dos Campos
Departamento de Engenharia de Controle e Automação

1. Nome do projeto

Identificação de teclas a partir da vibração resultante do pressionamento.

Membros da equipe

a. Aguinaldo Cardozo da Costa Filho
b. João Sinohara Silva Sousa
c. Renam Silva
d. Rodrigo Lantyer

2. Objetivos

O objetivo geral do projeto é expor a ameaça de identificação de senha em dispositivos equipados com unidades de medidas inerciais [1] como acelerômetros e giroscópios.

Os objetivos específicos incluem:

- a construção de um conjunto de treinamento;
- desenvolvimento, otimização, implementação, avaliação de uma rede neural artificial para realizar a predição de teclas pressionadas usando como entrada sinais capturados pelo acelerômetro/giroscópio. A plataforma de desenvolvimento com um embarcado de baixo consumo de energia, o Arduino Nano 33 Sense, será empregada para aquisição de dados e implementação do modelo.

3. Descrição do Projeto

Para atingir o objetivo definido, será desenvolvido uma prova de conceito empregando a plataforma de desenvolvimento Arduino Nano 33 Sense [2] para aquisição de sinais de vibração produzidos ao pressionar um teclado numérico emulado. O projeto será desenvolvido nas etapas mostradas na Figura 1 e discutidas a seguir:

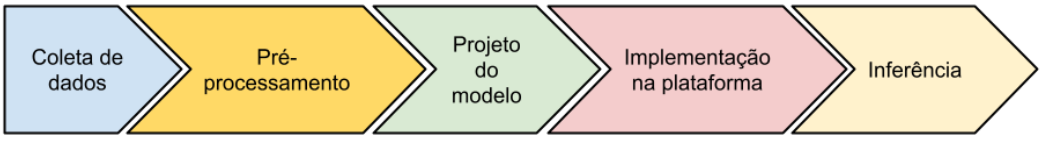

Figura 1 - Esquemático das etapas do projeto

- **Coleta de dados:** essa etapa consiste na coleta de sinais de vibração produzidos ao pressionar um teclado numérico de 0 a 9. O projeto busca confirmar ou refutar a ideia de que o pressionamento de cada tecla produz um padrão de vibração característico que pode ser explorado para discriminar a tecla pressionada. Naturalmente, essa possibilidade torna real a ameaça de revelação de dados sensíveis, como, por exemplo, senhas e votos depositados em urnas eletrônicas. Um ataque como o descrito, seria possível fixando um dispositivo eletrônico equipado com unidade de medidas inerciais no equipamento alvo do ataque ou explorando a disponibilidade da unidade no próprio dispositivo. Ideias similares já foram exploradas anteriormente na literatura técnica. Em [3] é exposta a ameaça de revelação de senha em fechaduras eletrônicas usando a vibração produzida no pressionamento de teclas. Após adquiridos, os sinais são enviados para uma unidade de processamento para inferência da senha. O trabalho [4] explorou o som, captado pelos microfones, produzido pelo acionamento de teclas virtuais em *smartphones* e *tablets* para inferir senhas e palavras digitadas.
- **Pré-processamento:** os sinais serão pré-processados para eliminação de erros da aquisição, checagem da consistência, anotação de rótulos e formatação para consumo no treinamento do modelo. Além disso, serão exploradas transformações/operações nos sinais com o objetivo de produzir uma representação mais adequada para a tarefa de classificação.
- **Projeto do modelo:** a etapa de projeto seguirá de forma iterativa, alternando entre projeto da arquitetura, treinamento do modelo e avaliação do desempenho. O objetivo é produzir um modelo equilibrado em termos de desempenho e recursos empregados, tendo em vista que o modelo final a ser embarcado na plataforma de Arduino Nano 33 Sense. O projeto da arquitetura inclui a definição do número de camadas, não linearidades/funções de ativações empregadas, quantidade/tamanho dos filtros, entre outros aspectos da arquitetura do modelo. Em seguida, o modelo será otimizado para minimizar a função objetivo usando pares de entrada/saída do conjunto de treinamento. O modelo treinado será avaliado no conjunto de validação e as métricas de desempenho serão usadas para realizar ajustes no modelo.
- **Implementação na plataforma:** essa etapa consiste em converter e embarcar o modelo resultante da conversão na plataforma Arduino Nano 33 Sense.
- **Inferência:** a plataforma Arduino Nano 33 Sense embarcada com o modelo final será usada para realizar inferência em sinais novos.

4. Descrição

a. Diagrama de blocos

A Figura 2 exibe um diagrama com blocos funcionais para implementar a solução. Ressalta-se que o diagrama está sujeita a alterações ao longo da implementação, o diagrama atual reflete o estágio de planejamento.

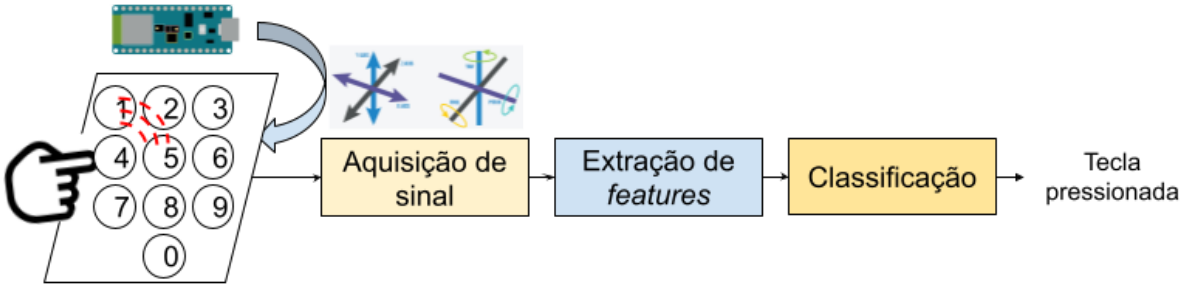

Figura 2 - Diagrama de blocos genérico da solução

b. Hardware

A Figura 3 mostra o esquemático da montagem da prova de conceito. A montagem consiste de uma plataforma sobre a qual estão distribuídas espacialmente teclas de 0 a 9 e da plataforma Arduino Nano 33 Sense que irá capturar a vibração e realizar a inferência das teclas pressionadas.

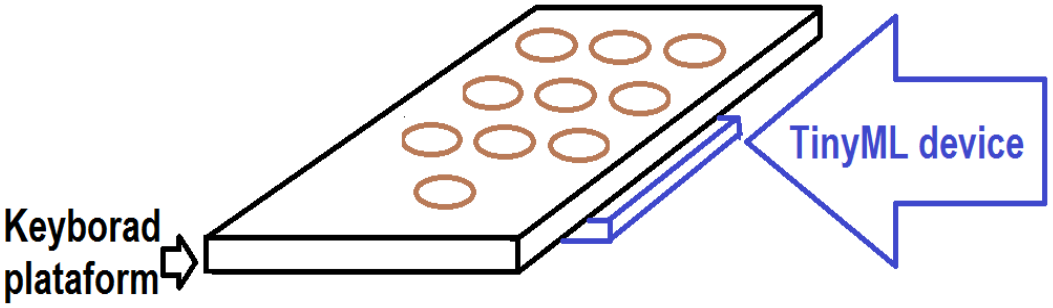

Figura 3 - Esquemático da montagem da prova de conceito

c. Conjunto de dados

Para o desenvolvimento do projeto será necessário realizar a aquisição da vibração produzida pelo pressionamento de cada tecla empregando o acelerômetro e/ou giroscópio disponível na plataforma Arduino Nano 33 Sense e fixada na plataforma de teclado. Para criar um conjunto de amostras diversificado e representativo da distribuição do sinal vibratório, a aquisição será realizada em várias etapas, com algumas variações na configuração. As variações previstas incluem a utilização de diferentes usuários, níveis de pressão, posicionamento da plataforma Arduino Nano 33 BLE Sense, entre outras que contribuam para a diversificação do conjunto de dados.

d. Pré-processamento

Como discutido anteriormente, os sinais serão pré-processados para garantir a consistência do volume de dados tanto para treinamento quanto para validação. Além disso, serão exploradas transformações/operações nos sinais com o objetivo de produzir uma representação mais adequada para a tarefa de classificação, como o uso dos sinais no domínio da frequência e utilizar técnicas que explorem melhor a separação de classes desse conjunto de recursos.

e. Projeto do modelo

No atual estágio do projeto, pode-se afirmar que será empregada uma rede neural artificial *feedforward.* Nas camadas iniciais que realizam a extração de características poderão ser empregadas unidades totalmente conectadas ou unidades convolucionais em que os pesos são compartilhados entre neurônios. Sem perda de generalidade, as camadas iniciais da arquitetura exibida na Figura 4 empregam unidades totalmente conectadas. Após a extração de *features,* a representação produzida é geralmente empilhada para alimentar camadas totalmente conectadas que realizam a classificação. No caso em particular do projeto, a etapa de classificação irá produzir a probabilidade de o sinal ter sido originado no pressionamento de cada uma das teclas disponíveis no teclado, ou seja, o classificador irá produzir um vetor de probabilidade. A classe predita será aquela com maior probabilidade.

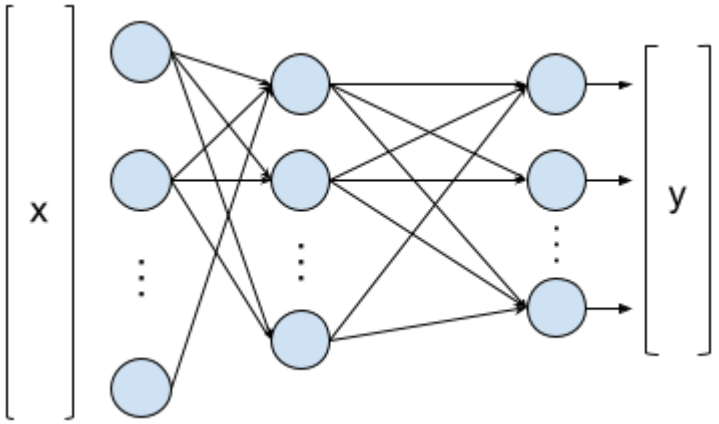

Figura 4 - Arquitetura genérica da rede a ser explorada

f. Otimizações

Como discutido anteriormente, o modelo será sujeito a várias etapas de otimização e aprimoramento. Alternando entre projeto da arquitetura, treinamento do modelo e avaliação do desempenho.

g. Modelo em modo de produção

A solução final composta da plataforma Arduino Nano 33 BLE Sense e o modelo treinado embarcado na plataforma será usado para realizar inferências sobre novos sinais capturados. Reafirmando o objetivo, a ideia é expor a possibilidade de ataques que revelem dados sensíveis de usuários quando estes pressionam teclas. A pressão exercida sobre a tecla inevitavelmente produz vibrações que podem ser exploradas, bastando apenas a utilização de unidades de medidas inerciais, como acelerômetros e giroscópios, e um microcontrolador executando uma rede neural artificial.

5. Desafios/obstáculos previstos e soluções potenciais

Os desafios e obstáculos identificados até o momento são descritos a seguir, juntamente com possíveis formas de mitigação ou evidência anteriores.

-Conjunto pouco representativo

a. aumentar a coleta de dados

- Inexistência de padrões vibratórios que possibilitem a discrimanação da tecla pressionada
    b. pesquisas anteriores sugerem que existe um padrão

6. **Maior questão não resolvida**
   Não foram identificadas questões que impossibilitem a implementação do projeto.

7. **Referências**

[1] Howtomechatronics, https://howtomechatronics.com/how-it-works/electrical-engineering/mems-accelerometer-gyrocope-magnetometer-arduino/

[2] https://www.arduino.cc/en/Guide/NANO33BLESense

[3] Youngmok Ha, Soo-Hee Jang, Kwang-Won Kim, Ji Won Yoon, “Side channel attack on digital door lock with vibration signal analysis: Longer password does not guarantee higher security level”, *IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, Daegu, Korea, 2017.

[4] Ilia Shumailov, Laurent Simon, Jeff Yan, Ross Anderson, "Hearing your touch: A new acoustic side channel on smartphones”, preprint https://arxiv.org/abs/1903.11137 (https://www.cl.cam.ac.uk/~is410/Posters/hearing_touch_poster.pdf)

[5]https://www.hackster.io/news/building-an-rf-side-channel-attack-using-machine-learning-6544e691542e

[6] https://elie.net/blog/security/hacker-guide-to-deep-learning-side-channel-attacks-the-theory/

[7] https://www.tau.ac.il/~tromer/handsoff/

[8] Vijay Janapa Reddi *et al.*, “Widening Access to Applied Machine Learning with TinyML”, preprint https://arxiv.org/abs/2106.04008