

DATILOSCOPIA PARA SISTEMAS EMBARCADOS

Gabriel Martinelli Dias (PIBIC/CNPq/FA/Uem), e-mail: ra79335@uem.br,
Elvio Joao Leonardo (Orientador), e-mail: ejleonardo@uem.br.

Universidade Estadual de Maringá, Centro de Tecnologia, Maringá, PR.

Ciências Exatas e da Terra – Ciência da Computação – Sistemas de Computação

Palavras-chave: Datiloscopia, Sistemas embarcados, Biometria

Resumo:

O projeto tem como objetivo a realização de um estudo e desenvolvimento de um sistema de controle de acesso por meio de verificação biométrica baseado em datiloscopia, ou seja, a identificação de indivíduos é realizada através de impressões digitais. Ao final do projeto foi desenvolvido um protótipo do sistema que cumpre com os objetivos, sendo utilizado a plataforma Arduino e um sensor óptico de impressão digital.

Introdução

A biometria é a técnica de reconhecimento de uma pessoa com base nas suas características fisiológicas, ou seja, a identificação é realizada a partir dos dados físicos ou comportamentais do indivíduo, tais como, impressões digitais, íris, geometria da mão, reconhecimento da face, voz e entre outros. Tal método de identificação passou a ser muito utilizado, pois, apresenta diversas vantagens demonstrando-se muito seguro, já que, utiliza-se de características que todas as pessoas possuem e as distinguem de todas as outras mantendo-se com essa individualidade para o resto da vida.

A impressão digital é o desenho formado por pequenas elevações na pele, também conhecida como papilas dérmicas, que se encontram nas pontas dos dedos, determinando as cristas e vales. Esse desenho formado por essas cristas e vales possuem as particularidades conhecidas como minúcias que se distinguem dos outros indivíduos, são essas as características utilizadas para fins de reconhecimento há muito tempo como uma forma de identificação biométrica, por causa da sua simplicidade e precisão.

O sistema de biometria visa solucionar problemas relacionados a controle de acesso de pessoas através de sistemas embarcados de baixo custo que contêm funções biométricas, considerando a economia de energia. Além disso, nota-se uma crescente demanda por sistemas automáticos que realizam esse controle, pois, oferecem uma maior segurança e confiabilidade.

Materiais e métodos

A metodologia do projeto se deu por estudos de algoritmos utilizados em datiloscopia em conjunto com o desenvolvimento da programação do Arduino Uno R3 (ARDUINO, 2017) e o sensor biométrico da AdaFruit (ZFM-20 Series Fingerprint Identification Module, 2018). Os estudos foram dirigidos ao software distribuído e desenvolvido pelo *National Institute of Standards and Technology* (NIST) para o *Federal Bureau of Investigation* (FBI) e *Department of Homeland Security* (DHS), pois, dispõe de código aberto, diferentemente do sensor biométrico ZFM-20 utilizado no projeto. Desta maneira, auxiliando o entendimento do sensor biométrico compreendendo a parte de processamento da imagem da impressão digital, reconhecimento de minúcias e comparação de digitais. As ferramentas do NIST estão distribuídas entre os seguintes pacotes:

- MINDTCT: sistema de reconhecimento de minúcias.
- BOZORTH3: sistema de *matching*.
- PCASYS: sistema de classificação que possibilita distinguir uma impressão digital em 5 grandes categorias.

O sensor ótico de impressão digital é o principal módulo utilizado, pois, é nele que ocorrerá todas as funcionalidades referente a biometria e processamento de imagem. O sensor possui os seguintes princípios de operações:

- Registrar um novo usuário: para cadastrar uma nova impressão digital necessita-se realizar a leitura do dedo duas vezes, então o sistema irá processar às duas imagens obtidas e gerar um modelo do dedo com base nos resultados do processamento.
- Correspondência: o usuário entra com dedo através de sensor óptico e ele irá gerar um modelo do dedo e compará-lo com modelos armazenados na memória flash.

A Figura 1 representa como é realizado o registro de um novo usuário no sistema.

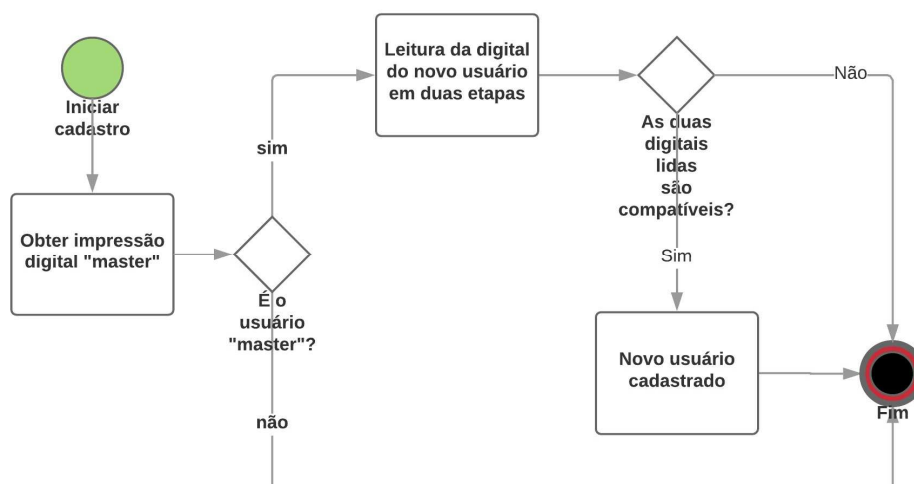


Figura 1 – Fluxograma do cadastro de usuário.

A Figura 2 representa a realização da correspondência em um fluxograma.

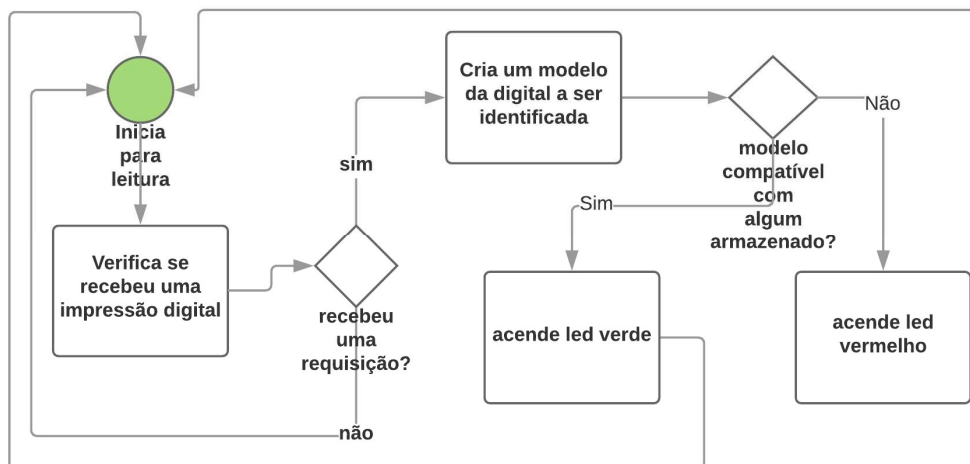


Figura 2 – Fluxograma de Correspondência do usuário.

Resultados e Discussão

Ao final foi desenvolvido um protótipo que contém as funcionalidades para cadastrar usuário e liberar entrada, onde os resultados obtidos desse controle de acesso foram satisfatórios, respeitando os objetivos de criar um sistema que seja pequeno, de baixo custo e de baixo consumo energético.

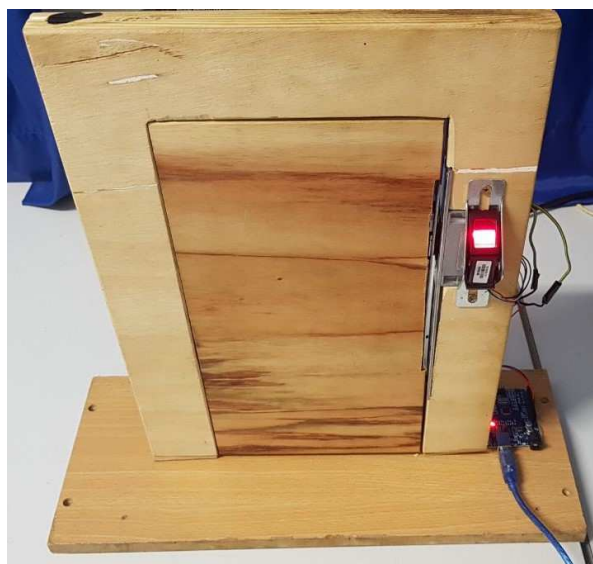


Figura 3 – Protótipo, visão frontal.

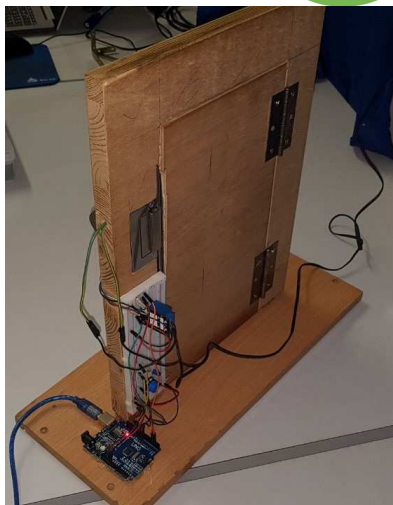


Figura 4 – Protótipo, visão traseira.

Conclusões

As conclusões obtidas neste projeto foram a respeito da complexidade de desenvolver algoritmo baseado em datiloscopia, uma vez que não existem soluções semelhantes disponíveis nas comunidades de hardware e software livres. Mesmo com as dificuldades, foi desenvolvido um sistema embarcado que realiza o controle de acesso com o uso de impressões digitais.

Para trabalhos futuros ao sistema torna-se possível inserir facilmente uma bateria para que atue de maneira ininterrupta, mesmo com queda de energia elétrica. Também seria relevante a criação de um *log* para armazenar as entradas dos usuários e algumas melhorias na questão da interface para facilitar a interação.

Agradecimentos

Agradecimentos ao CNPq, a Fundação Araucária e a UEM pelo apoio financeiro.

Referências

ARDUINO, disponível online em www.arduino.cc, acesso em 27/07/2018.

MALTONI, D. **Handbook of Fingerprint Recognition**. 2ª ed. New York: Springer-Verlag, 2009. 348 p.

NIST Fingerprint, disponível online em www.nist.gov/programs-projects/fingerprint, acesso em 27/07/2018.

ZFM-20 Series Fingerprint Identification Module, disponível online em www.olimex.com/Products/Components/Sensors/SNS-FINGERPRINT/resources/ZFM-user-manualV15.pdf, acesso em 27/07/2018.