SISTEMA DE CONTROLE DE ACESSO COM TRÊS FATORES DE AUTENTICAÇÃO PONTO DE CONTROLE 4

Mateus Felipe Massa, Victor Bastos I. Oliveira

Programa de Graduação em Engenharia Eletrônica, Faculdade Gama
Universidade de Brasília
Gama, DF, Brasil
email: mateusmassa7@gmail.com, victorbio101@gmail.com

RESUMO

Fazendo uso de uma placa Raspberry Pi, este projeto consiste no desenvolvimento de um sistema de controle de acesso com três fatores de autenticação, sendo estes a verificação de senha, checagem por RFID e reconhecimento facial por câmera. O sistema visa ser empregado em salas onde o acesso deve ser extremamente restrito, o que é relativamente comum no ramo de empresas laboratoriais, empresas de segurança, órgãos governamentais de alto escalão e forças armadas, por exemplo.

1. INTRODUÇÃO

Controle de acesso é definido como a prática de permitir a entrada e saída de um local apenas para indivíduos autorizados, a fim de garantir a segurança do conteúdo localizado na área. Este tipo de tecnologia tem aplicação em qualquer tipo de local que necessite da filtragem no acesso das pessoas, seja por questões de confidencialidade ou questões de segurança. A aplicação desse sistema pode ser exemplificada através de uma usina termonuclear, onde o acesso a certas partes críticas da planta deve ser estritamente controlado para evitar que pessoal não autorizado, geralmente sem conhecimento técnico e licenciamento, cause algum distúrbio e leve uma catástrofe à acontecer. Outro exemplo advém das aplicações governamentais e militares, onde segredos de Estado, arquivos de alto sigilo e equipamentos devem ser guardados com extrema cautela, com acesso liberado a apenas um seleto grupo de pessoas.

A motivação por trás desta proposta de projeto é realizar o controle eletrônico através de um dispositivo de segurança, mostrando que é possível criar um sistema complexo de autenticação e alerta que garante a eficiente filtragem do acesso de pessoal, a partir da combinação de diversos componentes e técnicas em eletrônica.

Alguns sistemas já propostos foram analisados para embasar o projeto em questão. Estes sistemas eram responsáveis por implementar uma trava inteligente à portas, a fim de garantir mais segurança ao usuário. No sistema proposto em [1] foi criado uma trava de segurança baseada na placa raspberry pi, utilizando câmeras e teclado matricial, para prover um sistema de alarme que tem capacidade de notificar o dono e reconhecer as faces dos usuários cadastrados. Em outro projeto, proposto em [2], foi feito o design e implementação de um sistema de monitoramento remoto de uma porta, a partir de um algoritmo de reconhecimento facial feito através da biblioteca OpenCV associado à checagem de senha, utilizando a raspberry pi como processador central. Em [3] foram implementados três métodos em sequência para validação da entrada, utilizando tecnologia RFID, uma senha PIN de seis dígitos e um código aleatório de único-acesso enviado como mensagem para o celular do usuário. Em todos os projetos tomados como base, nenhum implementou autenticação por três fatores propriamente dito, já que nenhum deles checou informações de tipos específicos na ordem necessária para ser classificado como autenticação por três fatores, como descrito em [4].

2. EXPERIMENTO

2.1. Descrição de Hardware

Na montagem inicial do sistema foram utilizados três principais hardwares, a fim de realizar uma prova de conceito para o projeto final. A placa raspberry pi 3 modelo B foi utilizada como unidade de processamento central, responsável por controlar os periféricos de acordo com o código embarcado, além de executar a primeira parte do controle de acesso. Para compilar e executar os arquivos/códigos necessários na placa foi utilizado acesso remoto através do programa VNC Viewer.

Conectado aos pinos da raspberry pi, o módulo RFID-RC522 foi utilizado como periférico para validação de acesso, agindo como o segundo fator em um sistema com três fatores de autenticação. Este módulo foi interfaceado com a placa através do protocolo de comunicação SPI, ocupando um total de cinco pinos, desconsiderando alimentação e aterramento. Duas tags padrão MIFARE1 S50, uma do tipo chaveiro e outra do tipo cartão, foram utilizadas para testar a funcionalidade do módulo. Em uma das portas USB da placa foi conectado uma webcam Logitech C270, de resolução máxima de 720p em 30 FPS. Este periférico foi utilizado para a checagem do último fator de autenticação, dado através do reconhecimento facial do usuário. Um display LCD 20x04, interfaceado com a placa através do protocolo de comunicação I2C, foi utilizado para repassar informações necessárias do sistema para o usuário.

2.2. Descrição de Software

O software embarcado no sistema foi constituído por dois blocos principais: um bloco de pré-processamento da imagem para o banco de dados e o bloco de controle de acesso com autenticação por três fatores (senha, RFID e reconhecimento facial).

O fluxograma abaixo descreve em mais detalhes o fluxo da informação dentro do programa do primeiro bloco:

Fig. 1. Fluxograma pré-processamento

No primeiro bloco utilizou-se principalmente a biblioteca OpenCV, uma biblioteca desenvolvida para processamento de imagens no geral. O caminho básico do programa pode ser dado pelo carregamento da imagem salva no banco de dados, o processamento da imagem para ajustá-la aos conformes necessários e por fim o salvamento da imagem, sobrescrevendo o arquivo original.

De começo a imagem é carregada em uma variável, a partir da leitura dela na pasta do banco de dados. Após isso, a imagem é levada através de um caminho de processos a fim de ser condicionada para facilitar o

processo de reconhecimento facial. No processamento da imagem têm-se os seguintes processos:

- Conversão em escala de cinza: converte a imagem em escala de cinza;
- Equalização de histograma: equaliza a imagem ajustando o contraste dela;
- Detecção de face e olhos: detectar na imagem processada face e olhos;
- Alinhamento dos olhos: a partir da detecção dos olhos, determina pontos de referência e alinha os olhos para deixar o rosto em um perfil totalmente frontal;
- Rotação da imagem: rotacionar imagem tomando como referência central o olho esquerdo;
- Remapeamento: remapeamento da imagem a partir de operações matemática para ajuste da mesma após a rotação;
- Corte: cortar a imagem selecionando somente a face;
- Redimensionamento: redimensionar imagem a partir de uma resolução gráfica definida;

Após o processamento o passo final é salvar a imagem, sobrescrevendo o arquivo original de modo que o programa de reconhecimento facial faça o treinamento do código com as imagens pré-processadas.

O bloco do controle de acesso foi desenvolvido utilizando como base a biblioteca MFRC522, uma biblioteca desenvolvida para o uso do módulo RFID na Raspberry Pi, uma função a parte de reconhecimento facial, desenvolvida a partir da biblioteca OpenCV, e utilizando funções prontas de uma biblioteca para o display LCD, desenvolvida em C com base na biblioteca wiringPi. O loop principal começa realizando a leitura de um arquivo de extensão csv que aponta o caminho do banco de dados com as imagens pré-processadas, depois é escolhido o método de reconhecimento facial (que no caso deste projeto foi utilizado o método Fisher Faces) e feito o treinamento do código a partir das imagens do banco de dados. Após isso, é feito o recolhimento de dados do usuário a partir do banco de dados, prosseguindo para a etapa das autenticações, sendo verificado as tentativas em cada fator de modo que se o usuário errar três vezes a verificação de senha ou da tag do RFID, o programa é finalizado. Já para a autenticação da face foi utilizada a função de reconhecimento citada, onde também foi verificado o número de tentativas, que nesse caso foi escolhido um número experimental que resultasse em espaço amostral de tamanho razoável. A principal verificação dessa etapa foi dada a partir do contador de sucesso que foi atrelado ao grau de confiabilidade da predição feita baseada na imagem pré-processada, de modo que se o grau for maior que 50% o contador de sucesso é incrementado e caso esse contador seja maior ou igual a quinze, a verificação é dada como correta e o usuário está liberado. Caso o número de tentativas chegue ao limite e o contador de sucesso não passe do limiar estabelecido a verificação é dada como falha, barrando a entrada do usuário.

O fluxograma abaixo descreve o funcionamento do programa descrito acima:

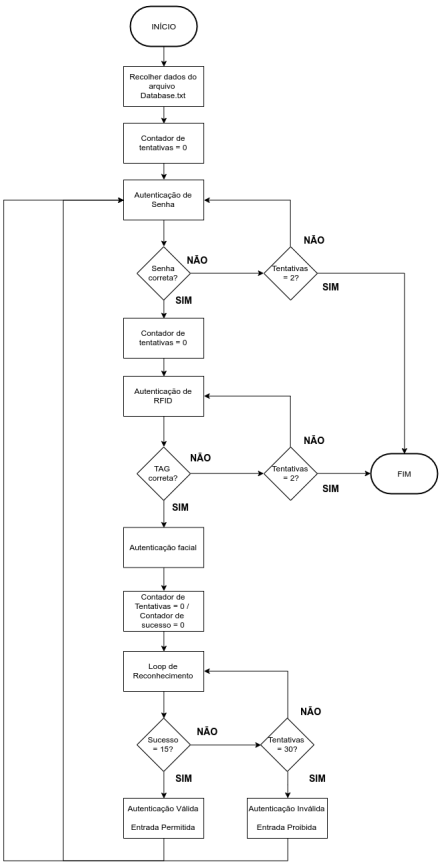

Fig. 2. Fluxograma Access Control

A função de reconhecimento citada acima é uma função a parte, desenvolvida utilizando a biblioteca OpenCV.

O funcionamento é dado a partir de um loop de tentativas onde o retorno é booleano indicando se a verificação foi verdadeira ou falsa. Nesta função têm-se a captura do quadro pego pela webcam e um processamento para comparação com as imagens do banco de dados, que consiste em colocar a imagem em escala de cinza, detectar face na imagem, cortar imagem em torno da face detectada e redimensionar imagem para uma resolução gráfica definida. A partir desse processamento é feito uma predição, que reconhece a face na imagem, gerando também um grau de confiabilidade dessa predição. A partir desses dois valores são feitas verificações, na qual, caso o identificador da predição seja igual a um identificador definido e o grau de confiabilidade seja maior que 50%, um contador de sucesso é incrementado, caso contrário o programa segue e um contador de tentativas é incrementado. A verificação final é baseada nesses dois contadores, onde, caso o contador de sucesso seja igual a quinze, a função retorna booleano verdadeiro, indicando que a autenticação foi um sucesso. Caso o contador de tentativas seja maior ou igual a vinte e a verificação anterior for falha, a função retorna booleano falso, indicando que a autenticação falhou.

O fluxograma abaixo demonstra o funcionamento da função descrita acima:

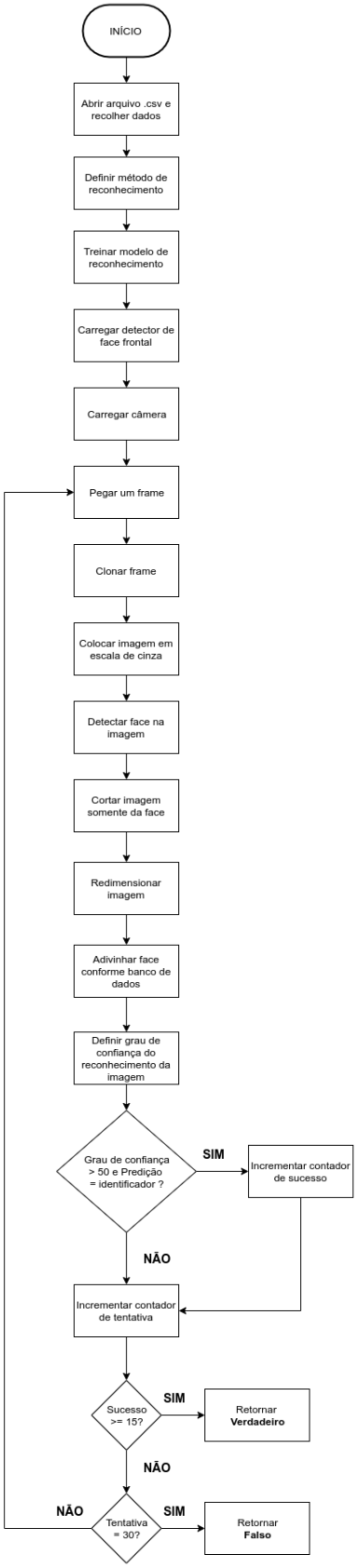

Fig. 3. Fluxograma Face Recognition

3. RESULTADOS

3.1. Resultados Preliminares

Com a configuração de hardware inicial e códigos de autenticação integrados, os resultados obtidos foram satisfatórios como parte do objetivo final. O primeiro fator de autenticação, uma senha numérica qualquer de seis caracteres, foi testado e validado com sucesso para a introdução de senhas com quantidade de caracteres acima e abaixo de seis. Ao entrar com uma senha diferente das duas cadastradas, o programa imprimiu no display que a senha estava incorreta e exigiu uma nova inserção de senha. Ao acertar a senha o programa passou para o próximo estágio de autenticação, carregando o número identificador de usuário cadastrado. O sistema RFID também foi testado e validado com sucesso. Ao passar a tag do tipo incompatível com o número identificador de usuário o acesso foi negado, porém ao passar a tag do tipo correto o acesso foi liberado e o programa avançou para o estágio de reconhecimento facial. Neste último fator o programa de reconhecimento foi executado certa quantidade de vezes, detectando a face e realizando o prognóstico do reconhecimento quadro por quadro. A autenticação falhou quando uma pessoa diferente da cadastrada com o número identificador sendo analisado foi reconhecida. Quando a pessoa correta era reconhecida, o programa entendia que os três fatores haviam sido cumpridos e escrevia no display uma mensagem de boas vindas.

4. REFERENCIAS

[1] V. MISHRA, Shwetank. SONI, "Smart door system for home security using raspberry pi 3." [Online]. Available: http://ijirt.org/master/publishedpaper IJIRT146080_PAPER.pdf

[2] N. e. a. ROY, Sourav. UDDIN, "Design and implementation of the smart door lock system with face recognition method using the linux platform raspberry pi." [Online]. Available: http://ijcsn.org/IJCSN-2018/7-6/Design-and-Implementation-of-the-Smart-Door-Lock-System-with-Face-Recognition-Method-using-the-Linux-Platform-Raspberry-Pi.pdf

[3] S. O. NETWORK, "Build a raspberry pi smart door lock security system for your smart home." [Online]. Available: https://bit.ly/2NDopdM

[4] M. ROUSE, "Three factor authentication (3fa)." [Online]. Available: https://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA