

Sistema de segurança com reconhecimento facial - Acesso a locais restritos em bancos

Matheus Moreira da Silva Vieira
Universidade de Brasília,
Faculdade do Gama — UnB, FGA
Matrícula: 14/0155546
Email: matheus.silvadf@gmail.com

Saulo Alves Lisboa
Universidade de Brasília,
Faculdade do Gama — UnB, FGA
Matrícula: 13/0145262
Email: saulo_llisboa@hotmail.com

Abstract—Este projeto visa criar um protótipo de reconhecimento facial utilizando webcam proporcionando segurança e acesso restrito a locais que sejam necessário em bancos como salas confidenciais com auxílio da raspberry pi.

Raspberry Pi, microcomputador, automação, reconhecimento facial, controle de acesso, opencv.

I. REVISÃO BIBLIOGRÁFICA

A. Reconhecimento Facial

O reconhecimento facial é uma importante área vinculada ao reconhecimento de padrões que utilizam técnicas avançadas de processamentos de sinais e imagens através de métodos biométricos estando presente em diversas aplicações. (THEODORIDIS; KOUTROUMBAS, 2009) A identificação de um rosto feita pelo cérebro humano se dá pela forma natural e instantânea da pessoa no qual, através da memorização dos olhos, boca, nariz, cabelo há o reconhecimento da pessoa havendo a identificação da mesma. O processo de reconhecimento é realizado a partir de pontos de medida do rosto, que fazem uma ligação algorítmica de traços e tamanhos, como exemplo pode-se citar a distância exata entre nariz e orelhas, tamanho do crânio, arcada dentária, entre outros detalhes.



Fig. 1. Identificação de pontos no rosto humano.

A tecnologia de reconhecimento facial pode ser aplicada em diversas ocasiões distintas, sendo o principal mercado hoje relacionado à segurança, no entanto há uma variedade de aplicativos relacionados ao uso pessoal, aumento de produtividade, entre outros. Aplicativos detectam as faces das pessoas no vídeo em tempo real contra as bases de dados das imagens para encontrar a pessoa conhecida.

B. OpenCV

O processamento de imagem tem ganhado avanços no decorrer dos anos, novas ferramentas são criadas para facilitar o desempenho da imagem, seja na captura ou na qualidade. Entre os estudos de processamentos de imagens foram criadas plataformas que ajudam no melhoramento da detecção da imagem entre elas a ferramenta OpenCV. O OpenCV é uma ferramenta de processamento de imagens na qual possui uma biblioteca multiplataforma podendo ser programado em C/C++, Python, Visual Basic, Ruby facilitando o desenvolvimento para o software embarcado.

A biblioteca OpenCV permite a manipulação de dados de imagens, manipulação de matrizes e vetores, desenvolvimento de rotinas de álgebra linear, estruturas de dados dinâmicas, desenvolvimento de algoritmos de processamento de imagem, análise de movimento (tracking), reconhecimento de objetos, GUI básica e rotulagem de imagem.[1]

C. Empresas que oferecem serviços com reconhecimento facial

Já existem inúmeras empresas no mercado que utilizam a tecnologia de reconhecimento facial. A seguir serão listadas três exemplos. A primeira é a *idwall*. De acordo com o site da empresa sua tecnologia de reconhecimento reduz o risco de fraudes por personificação. Através da comparação de uma foto tirada no momento do cadastro e a foto usada no documento, confirmam que seus usuários são quem realmente eles dizem ser.



Fig. 2. Imagem fornecida pelo site da idwall.

Também existe a *CredDefense*. É possível encontrar no site da empresa a seguinte explicação: é uma plataforma de

biometria facial operando em nuvem. A empresa processa uma combinação de dados biométricos transformando cada face em um código único, que é criptografado e armazenado em um banco de dados centralizado. As informações resultantes, disponibilizadas em segundos, combatem tentativas de fraude, autenticam transações e simplificam processos, tornando-os mais ágeis e seguros.



Fig. 3. Imagem fornecida pelo site da CredDefense.

A empresa mais próxima com a proposta do projeto é a *MADIS*. Conforme escrito no site da empresa, é uma empresa especializada em fornecer tecnologia de ponta para Biometria Reconhecimento Facial, Relógio de Ponto e Controle de Acesso para Pessoas e Veículos.



Fig. 4. Produto de reconhecimento facial da empresa.

II. JUSTIFICATIVA

Existem muitos tipos de laboratórios, salas de informática, galpões, edifícios e entre outros lugares que guardam mercadorias ou objetos de grande valor comercial por exemplo: Notebooks, arquivos confidenciais, produtos eletrônicos,

medicamentos, dinheiro, equipamentos, ferramentas. Portanto, sempre é válido pensar e investir em maneiras de como proteger esses produtos em ambientes seguros. O acesso com o reconhecimento facial fica restrito apenas as pessoas cadastradas garantindo a segurança do local, além de evitar que possíveis invasores se utilizem de michas ou decidam danificar a fechadura.

III. OBJETIVOS

- Garantir o acesso apenas a pessoas autorizadas
- Desbloquear uma fechadura apenas com a identificação do rosto
- Garantir a segurança aos usuários

IV. REQUISITOS

- Uso do Raspberry Pi.
- Controle da entrada restrita apenas as pessoas cadastradas.
- Garantir o acesso com reconhecimento facial.
- Fornecimento de 3.3 V, 5 V e 12 V para o sistema;
- Bateria para o caso de falta de energia;
- Destravamento da trava magnética após o reconhecimento facial.

V. BENEFÍCIOS

- Tecnologia aplicada na segurança;
- Praticidade;
- Segurança em salas que abrigam bens de valor ou documentos;
- Segurança aos usuários;
- Acesso restrito a pessoas;

VI. VISÃO GERAL DO SISTEMA

O sistema funcionará da seguinte forma: O usuário terá seu rosto cadastrado na Raspberry Pi. O local de acesso restrito terá uma porta com uma trava magnética e uma câmera Webcam. O usuário, ao ser cadastrado terá que se aproximar da câmera webcam para o reconhecimento facial, o rosto será comparado com um banco de dados e, caso o rosto do usuário esteja de acordo com o rosto cadastrado destrancará a porta dando acesso ao lugar restrito. O lugar restrito, por exemplo, pode ser uma sala de documentos confidenciais ou a sala do cofre.

1) Lista de componentes necessários:

- Raspberry Pi3;
- Câmera Webcam;
- Trava magnética;
- Relês;
- Fontes de 3,3V, 5V e 12V com Nobreak;
- Botoeira temporizadora;

A. Descrição do Hardware

A integração geral do Hardware foi realizada fisicamente, visto que na figura a seguir obteve-se uma breve noção de como ficou a montagem dos componentes. Logo em seguida obteve-se a descrição de cada componente apresentada na Fig. 5 a seguir:

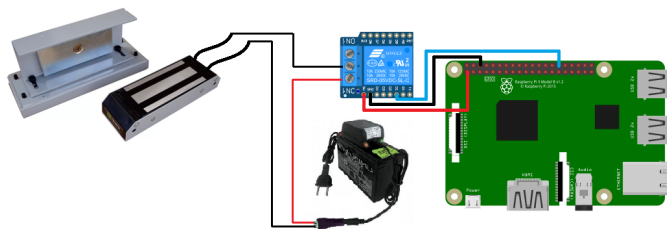


Fig. 5. Esquemático do hardware.

O pino de entrada foi conectado à GPIO5 da Raspberry Pi 3 para que fossem enviados os comandos para abrir a porta. Será usada uma fechadura eletroimã com kit universal de 150 kgf. A trava magnética funciona como um circuito normalmente fechado. Ela mantém a porta fechada até que se retire a tensão 12V em seus terminais. Quando isto acontece a corrente é interrompida, o campo magnético é cessado e a porta aberta. Um relé é necessário para controlar a fechadura pois sua operação é com 12V e o sinal do controlador é de 5V no máximo. A alimentação a ser utilizada é uma fonte 12V - 2.1A com nobreak para que, no caso de falta de energia, a porta não abra e desproteja o local. Uma botoeira temporizadora também foi adquirida para a abertura da porta pelo lado de dentro. Para o teste do hardware foi montado um circuito em protoboard com uma chave para simbolizar o estado do sistema. A Raspberry lê o estado da chave e envia um sinal para que a trava seja destrancada.

B. Descrição do Software

O projeto é composto por dois parâmetros: Detecção facial e Reconhecimento facial.

Detecção Facial: O primeiro passo para fazer um reconhecimento facial é a detecção facial. Nesse projeto foi feita a detecção facial utilizando o biblioteca Opencv e um arquivo chamado haarcascade. Nesse avanço do projeto foi feita a programação em c. Essa detecção é feita para saber se realmente há uma face posta na câmera para que o próximo passo seja o reconhecimento facial.

Reconhecimento Facial: Nesta segunda parte do projeto, o reconhecimento é feito utilizando a biblioteca *face-recognition* que tem por finalidade diferenciar de modo instantâneo a imagem da câmera da imagem cadastrada.

Feita a detecção facial utilizando a função haarcascade, o próximo passo necessário foi ter um banco de dados com o nome do usuário nos arquivos cadastrados para que, quando a câmera detectar a face, possa realizar os parâmetros de comparação e fazer a liberação da trava magnética. Foi acrescentado ao código a fase de construção do banco de dados, que consiste em tirar 25 fotos e salvá-las em uma pasta para que possa haver a comparação e, caso seja a pessoa cadastrada, execute o reconhecimento facial. Para facilitar a programação foi feita um fluxograma conforme a imagem a seguir.

Concluídas as fases de detecção facial e o cadastramento das fotos foi preciso um treinamento das imagens por parte do programa. O projeto seguiu para a fase de reconhecimento

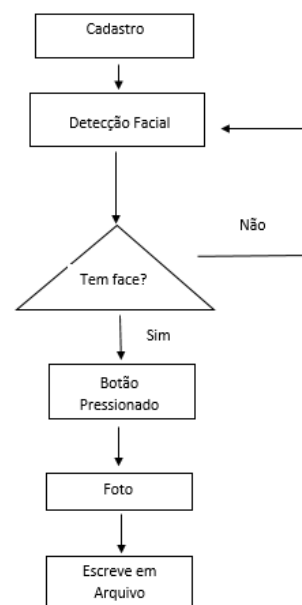


Fig. 6. Cadastro.

facial em si. Foram testados 3 tipos de reconhecedores: *EigenFace*, *FisherFace* e *LBPH*. Foi escolhido o *LBPH* (*Local Binary Patterns Histograms*) pelo seu nível de confiabilidade. Embora sua taxa de acerto seja menor seus acertos são mais precisos, além disso quando o reconhecedor errava considerava como desconhecido por um condicionador imposto no código, tornando o projeto mais confiável.

VII. RESULTADOS

Até o momento o projeto não está totalmente integrado, entre hardware e software. No entanto o software está funcionando razoavelmente com todas as partes: Construção do banco de dados, treinamento das imagens e reconhecimento em tempo real com certa faixa de segurança. As Fig. 7 e 8 mostram o reconhecimento em funcionamento. Foi montado a parte do hardware e funcionou como esperado. Na montagem foi utilizada uma chave sinalizando o sinal da câmera para que haja a abertura e o fechamento da trava de acordo com posicionamento da chave. De acordo com Fig. 9 abaixo pode-se verificar a montagem do hardware feita com sucesso. Para a conclusão do projeto falta apenas um refinamento do reconhecimento e a comunicação e integração com o hardware.

REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L^AT_EX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
- [2] SANTOS Barboza, Daniel Ponciano. Estudo da Biblioteca OpenCV. Universidade Federal do Rio de Janeiro - Escola Politécnica - Departamento de Eletrônica e de Computação. 2009
- [3] Silva Neto and JAMES Gomes. Métodos de Reconhecimento de Face Baseado em Estatística de Ordem Superior Lavras-MG. 2016.
- [4] Okabe, R. K. and Carro, S. A. Reconhecimento Facial em imagens capturadas por câmeras digitais de rede. 2015.
- [5] <https://idwall.co/face-match/>. Acesso em 05/09/2018.
- [6] <http://creddefense.com.br/>. Acesso em 05/09/2018.
- [7] <http://madis.com.br>. Acesso em 05/09/2018.

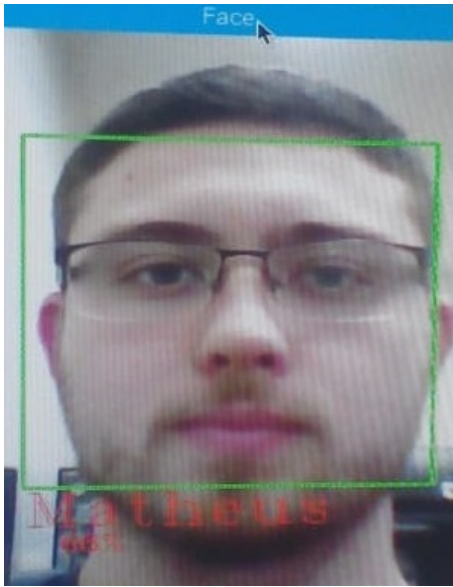


Fig. 7. Reconhecimento de um dos integrantes.



Fig. 8. Reconhecimento do outro integrante.

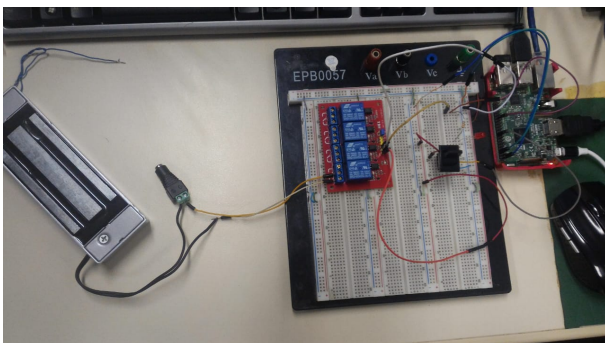


Fig. 9. Montagem.