UNIVERSIDADE DO VALE DO TAQUARI
CURSO DE ENGENHARIA DA COMPUTAÇÃO

AVALIAÇÃO DE EFETIVIDADE E ACEITAÇÃO DA TÉCNICA DE BIOMETRIA FACIAL PARA CONTROLE DE ACESSO EM UMA EMPRESA DE TECNOLOGIA DO VALE DO TAQUARI

Maurício Ribeiro Xavier

Lajeado, junho de 2021

Maurício Ribeiro Xavier

AVALIAÇÃO DE EFETIVIDADE E ACEITAÇÃO DA TÉCNICA DE BIOMETRIA FACIAL PARA CONTROLE DE ACESSO EM UMA EMPRESA DE TECNOLOGIA DO VALE DO TAQUARI

Monografia apresentada na disciplina de Trabalho de Conclusão de Curso, do curso de Engenharia da Computação, da Universidade do Vale do Taquari - UNIVATES, como parte da exigência para a obtenção do título de bacharel em Engenharia da Computação

Orientador: Prof. Me. Juliano Dertzbacher.

Lajeado, junho de 2021

RESUMO

O uso da tecnologia como uma alternativa para garantir uma maior segurança para as pessoas ou patrimônio privado já é uma realidade consolidada. Neste contexto, as câmeras de vigilância são fundamentais no combate a possíveis intrusos. Porém, designar a tarefa de controle e reconhecimento a um ser humano, especialmente em ambientes onde há muita circulação de pessoas, pode resultar em uma perda de eficiência. Desta forma, os sistemas de reconhecimento facial, através das imagens captadas por câmeras, podem servir como uma ferramenta para otimizar este processo. Considerando este cenário, o trabalho objetiva modernizar os sistemas de segurança de uma empresa, através do desenvolvimento de um sistema *web* de reconhecimento facial para realizar o controle da entrada de pessoas nas suas dependências. A aplicação desenvolvida conta com uma interface de acompanhamento por parte dos gestores da empresa, na qual poderão ser adicionadas ou removidas faces autorizadas, além da possibilidade de observar o histórico de novas faces reconhecidas. Através de um estudo acerca das técnicas empregadas em trabalhos relacionados ao campo de visão computacional foi possível expandir o embasamento teórico e constatar, a partir de testes com os colaboradores e gestores da empresa, que os resultados apresentados pela ferramenta desenvolvida foram satisfatórios, desempenhando de maneira eficaz o reconhecimento facial dos usuários.

Palavras-chave: Reconhecimento facial; Biometria; Controle de acesso.

ABSTRACT

The use of technology as an alternative to ensure greater security for people or private property is already a consolidated reality. In this context, surveillance cameras are essential in combating possible intruders. However, assigning the task of control and recognition to a human being, especially in environments where there is a lot people moving, can result in a loss of efficiency. Thus, facial recognition systems, through images captured by cameras, can serve as a tool to optimize this process. Considering this scenario, the work aims to modernize a company's security systems, through the development of a web-based facial recognition system to control the entry of people into its facilities. The developed application has an interface for monitoring by the company's managers, in which authorized faces can be added or removed, in addition to the possibility of observing the history of new recognized faces. Through a study of the techniques used in works related to the field of computational vision, it was possible to expand the theoretical basis and verify, from tests with employees and managers of the company, that the results presented by the developed tool were satisfactory, effectively performing users' facial recognition.

Keywords: Facial Recogntion; Biometrics; Access Control.

LISTA DE ILUSTRAÇÕES

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Program Interface*
DNA	*Deoxyribonucleic Acid*
FA	*False Acceptance*
FAR	*False Acceptance Rate*
FR	*False Reject*
FRR	*False Rejection Rate*
HD	*High Definition*
IP	*Internet Protocol*
JSON	*JavaScript Object Notation*
LFW	*Labled Faces in the Wild*
LBPH	*Local Binary Patterns Histograms*
LED	*Light Emitter Diode*
OpenCV	*Open Source Computer Vision Library*
PCA	*Principal Component Analysis*
PIR	*Passive Infrared Sensor*
REST	*REpresentational State Transfer*
RF	Requisitos Funcionais
RNF	Requisitos Não Funcionais

ROI	*Region Of Interest*
RTSP	*Real Time Streaming Protocol*
TA	*True Acceptance*
TAR	*True Acceptance Rate*
TR	*True Reject*
XML	*Extensible Markup Language*
YAML	*YAML Ain't Markup Language*

SUMÁRIO

1 INTRODUÇÃO

Há muitos anos as técnicas de reconhecimento de pessoas são fundamentais, no contexto da segurança, para controle de acesso. A cada dia essa necessidade é reforçada pelo aumento das taxas relacionadas ao crime, principalmente em países subdesenvolvidos ou emergentes como o Brasil.

De acordo com Jain, Boole e Pankanti (2005), a combinação entre uma identidade e uma pessoa caracteriza o conceito de identificação pessoal. Este conceito pode ser dividido entre a verificação (confirmação de uma identidade previamente assumida) ou reconhecimento (identificação através da atribuição de uma possível identidade a uma pessoa) de indivíduos.

Para que um sistema de controle de acesso seja eficiente, é muito importante que antes de sua implementação seja avaliado o nível de risco apresentado no local de aplicação, visto que presumir ameaças de alto nível em todas as situações, pode acabar diminuindo a performance dos sistemas quando as circunstâncias não exigem demasiadas validações (JACOBSON; KOBZA; NAKAYAMA, 2000).

Neste contexto, tecnologias como o reconhecimento através de impressões digitais ou leitura da íris são mais comumente encontradas, porém, ainda exigem a colaboração dos usuários para que possam atingir os seus propósitos. Desta forma, as técnicas de biometria facial, quando utilizadas em conjunto com sistemas de controle de acesso, apresentam-se como uma boa alternativa (RAMESWARI et al., 2020).

Niu e Chen (2018) afirmam que as técnicas de reconhecimento facial se comparadas a outros métodos que utilizam biometria se destacam pelo fato de não exigirem contato do indivíduo, não apresentarem comportamento invasivo e estarem em uma área caracterizada pela contínua expansão e desenvolvimento. Além disso, o fato de não haver a necessidade de participação do indivíduo no processo de identificação também é um fator determinante na proeminência desta tecnologia.

Desta forma, considerando a contextualização apresentada, este trabalho apresenta como proposta o desenvolvimento de uma aplicação *web* de reconhecimento facial para modernizar os sistemas de segurança relacionados ao controle de acesso em uma empresa de tecnologia.

1.1 Problema de pesquisa

A preocupação com a segurança de colaboradores, bem como do patrimônio privado, sempre foi um tema de bastante relevância dentro das organizações. Apesar da tecnologia já ter se consolidado como um aliado neste processo, através da utilização de câmeras de vigilância e alarmes, por exemplo, em muitos casos ainda é necessário que haja intervenção humana nestes equipamentos para que possíveis intrusos sejam detectados.

Neste sentido, apesar de muitas empresas possuírem todos os equipamentos necessários, ainda não dispõem de técnicas modernas e fundamentadas na automatização do controle de acesso em suas dependências. Este fato acaba criando a necessidade da utilização de práticas que não estão entre as mais recomendadas no contexto da segurança, como a distribuição de senhas entre os funcionários, por exemplo.

Tendo em vista este cenário, identifica-se o problema de pesquisa: o uso da biometria facial, aprimorando as ferramentas de segurança existentes, pode ser utilizado em definitivo para o controle de acesso às dependências da empresa?

1.2 Objetivos da pesquisa

Para que o problema possa ser resolvido, o trabalho tem como objetivo geral modernizar os sistemas de segurança utilizados por uma empresa de tecnologia, através do desenvolvimento de uma aplicação que empregará técnicas de reconhecimento facial para realizar o controle de acesso nas dependências da organização.

Para que o objetivo geral seja alcançado, os seguintes objetivos específicos foram definidos:

- Buscar e analisar algoritmos de biometria facial já existentes e que possuam alta taxa de assertividade;
- Desenvolver uma aplicação integrada com o software da empresa, que será responsável por verificar se uma pessoa possui ou não autorização para acessar as dependências do local;
- Avaliar a solução, garantindo uma assertividade de nível considerável, de maneira que esta aplicação possa efetivamente ser utilizada pela empresa;
- Avaliar a aceitação dos colaboradores em relação ao processo de reconhecimento facial.

1.3 Estrutura do trabalho

Para uma melhor compreensão deste trabalho, uma breve explicação de sua estrutura será abordada a seguir.

O capítulo de introdução trata de uma contextualização da importância que a segurança tem nos dias de hoje, como deve ser realizado o planejamento para a aplicação de um sistema de segurança e aborda a biometria facial como uma alternativa de aplicação para contornar os problemas relacionados ao fator humano

no controle destes sistemas. Além disso, também são estabelecidos o problema de pesquisa, objetivos gerais e específicos e estrutura do trabalho.

No segundo capítulo é apresentado o referencial teórico com o levantamento bibliográfico realizado para a compreensão do conteúdo de estudo. Inicialmente são abordados conceitos fundamentais como os sistemas de segurança, biometria e os sistemas biométricos. Posteriormente, é apresentado o conteúdo de reconhecimento facial e as técnicas e métricas empregadas por outros autores.

No terceiro capítulo são destacados alguns trabalhos relacionados ao tema de estudo, onde é feita uma relação destes com o trabalho atual para reforçar pontos importantes no desenvolvimento desta pesquisa.

O quarto capítulo expõe a abordagem metodológica empregada para a elaboração da proposta deste trabalho, destacando os métodos científicos, procedimentos metodológicos e ferramentas escolhidas para a elaboração do projeto.

No quinto capítulo são apresentados os resultados esperados, dificuldades identificadas e conclusões deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será apresentada a base teórica que compreende os conceitos pelos quais este trabalho está fundamentado. Serão abordados desde pontos gerais até conceitos mais específicos, para que o conhecimento relacionado à pesquisa possa ser abrangido de forma completa.

2.1 Sistemas de segurança para Controle de Acesso

Bakshi e Prabhu (2017) afirmam que o controle de acesso, definido pela fiscalização das entradas de uma casa ou escritório, se destaca como uma das principais áreas da segurança nos dias de hoje, dado o aumento contínuo nos casos de roubo a cada ano. Os autores acrescentam que os métodos tradicionais de controle de acesso, como chaves ou cartões identificadores não são mais confiáveis por poderem facilmente ser perdidos, extraviados ou roubados. Desta forma, os autores sugerem que os sistemas atuais de controle de acesso devem ser modernizados e apresentam como alternativa o uso das tecnologias biométricas como uma possível solução para fortalecer a segurança.

De acordo com Jacobson, Kobsa e Nakayama (2000) o controle de acesso, no contexto da segurança física de ambientes, caracteriza-se principalmente pela definição de um ponto para realizar o monitoramento da entrada de indivíduos em

um local. A partir deste ponto, é aplicado um controle que irá definir se uma pessoa terá permissão ou não para acessar determinada área.

Os autores ainda acrescentam que este tipo de sistema é bastante similar ao controle de qualidade de produtos aplicado em indústrias, visto que nestes casos uma checagem deve ser aplicada para certificar que os produtos defeituosos não cheguem até o cliente e gerem prejuízos para a empresa.

Para Souza (2010), o objetivo dos sistemas de segurança para controle de acesso está na análise da identidade de um indivíduo para posteriormente liberar ou não o seu ingresso em determinada área onde se deseja aplicar o monitoramento.

2.2 Biometria

Segundo Labati et al. (2016), o conceito de Biometria está diretamente relacionado a utilização de padrões de comportamento psicológicos e características físicas para realizar o reconhecimento de indivíduos. Para os autores, os traços biométricos se diferem de outros recursos, como senhas e tokens, pelo fato de serem únicos para cada usuário e não apresentarem riscos de roubo ou esquecimento por parte dos portadores.

A biometria possibilita a autenticação ou identificação de um indivíduo por meio da análise de dados biométricos como o rosto, impressões digitais, íris e voz, por exemplo. Estes dados são características únicas que podem ser reconhecidas como a identidade dos indivíduos analisados (MASONA et al., 2020).

Liu e Silverman (2001) afirmam que dentro do campo da segurança a biometria se destaca como a ferramenta de autenticação mais segura que pode ser aplicada, visto que os traços de uma pessoa não podem ser emprestados, esquecidos ou roubados e a adulteração de um traço é praticamente impossível. Além disso, os autores citam e comparam (Figura 1) alguns tipos de biometria:

- Impressões digitais: as impressões digitais podem ser encontradas em padrões da pele normalmente extraídos das pontas dos dedos. Este tipo de biometria é mais recomendado para sistemas de segurança aplicados em ambientes controlados onde os usuários podem receber treinamentos;
- Retina: compreende a análise da camada de vasos sanguíneos encontrados na parte de trás do olho. Esta biometria aplicada a um sistema de segurança consiste na aplicação de uma luz de baixa intensidade no olho para obter os padrões ímpares de cada retina.
- Iris: abrange a análise dos padrões encontrados no anel colorido que envolve a pupila do olho. Quando aplicada a um sistema de segurança, trata-se do método menos intrusivo das biometrias relacionadas ao olho, visto que não requer tanta proximidade entre o usuário e a ferramenta extratora dos padrões.
- Face: trata-se da análise das diferentes características do rosto humano. No contexto da segurança, este tipo de biometria exige uma câmera responsável por gerar uma imagem que posteriormente será utilizada para aplicar a autenticação de um usuário;
- Voz: este tipo de biometria na segurança não se caracteriza pelo reconhecimento da voz de um indivíduo e sim na análise dos sons emitidos convertidos em texto.

Figura 1 – Comparativo entre os tipos de biometria.

Table 1. Comparison of biometrics

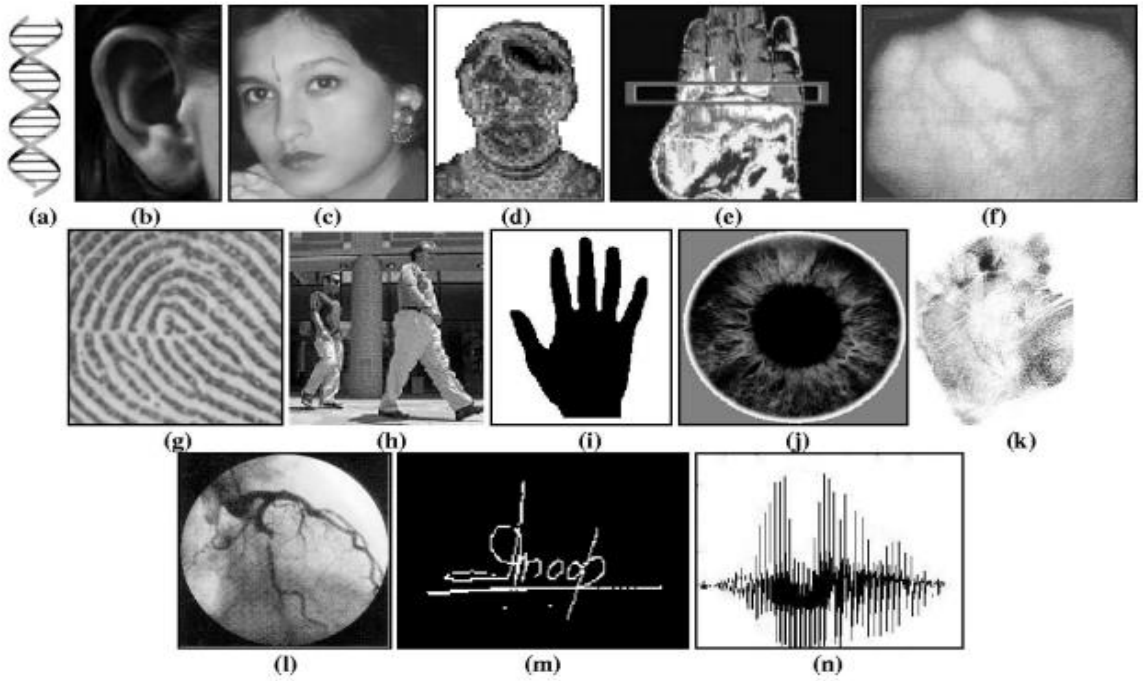
Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

Fonte: LIU e SILVERMAN, (2001).

No contexto dos tipos de biometria, Jain, Ross e Prabhakar (2004) afirmam que há diversos tipos de biometria (Figura 2) para muitas possibilidades de aplicações e que não há biometria perfeita para todos os cenários de aplicações possíveis, sendo assim, cada classe possui seus pontos fortes e fracos. Os autores ainda complementam que a combinação perfeita entre uma aplicação e um tipo específico de biometria depende dos requisitos operacionais da aplicação e dos atributos da característica biométrica em questão.

Figura 2 – tipos de biometrias: (a) DNA, (b) orelha, (c) face, (d) termograma facial, (e) termograma das mãos, (f) veias das mãos, (g) impressões digitais, (h) forma de andar, (i) geometria das mãos, (j) íris, (k) impressão palmar, (l) retina, (m) assinatura, (n) voz.



Fonte: JAIN, ROSS e PRABHAKAR, (2004).

2.2.1 Sistemas Biométricos

Segundo Jain, Ross e Prabhakar (2004), os sistemas biométricos atuam na obtenção de dados biométricos dos usuários, extração de um conjunto de características específicas destes dados e posteriormente os comparando com

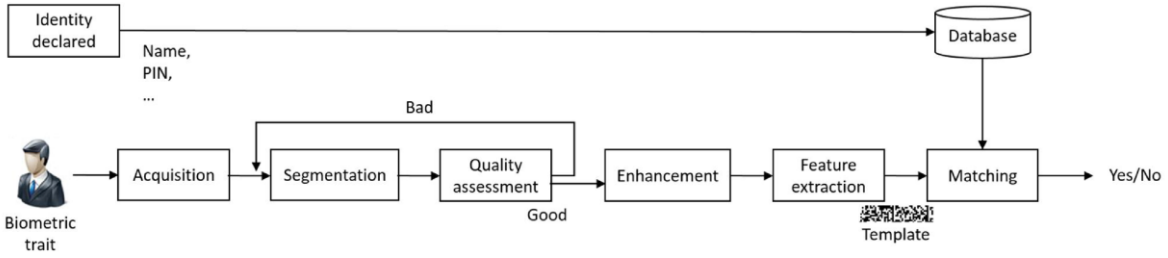
modelos pré-cadastrados em uma base de dados, podendo assim ser caracterizados como sistemas de reconhecimento de padrões.

Os sistemas biométricos possuem a função de identificar padrões de comportamento ou características físicas com a finalidade de avaliar a autenticidade de um indivíduo. Na maioria dos casos, estes sistemas são aplicados em situações em que se quer monitorar o acesso lógico ou físico a ambientes ou aplicações, confirmar a presença em compromissos, estabelecer a vigilância de um local ou garantir a aplicação da lei (LOZOYA-SANTOS et al., 2019).

De acordo com Labati et al. (2016), os sistemas biométricos são caracterizados pela integração de dispositivos, procedimentos e algoritmos com o objetivo de comparar as características de indivíduos para que seja possível determinar se estes pertencem a mesma pessoa. Os autores acrescentam que para atingir os resultados alguns passos são importantes (Figura 3):

- Aquisição (*Acquisition*): aplicação de um procedimento para adquirir de maneira digital um traço biométrico do indivíduo;
- Segmentação (*Segmentation*): etapa onde se separa somente a informação do traço biométrico;
- Avaliação de Qualidade (*Quality Assessment*): certificação para garantir que as informações obtidas são suficientes ou estão corretas;
- Aprimoramento (*Enhancement*): etapa onde a qualidade da amostra é aumentada;
- Extração de Características (*Feature Extraction*): as características distintas são então recolhidas e armazenadas em um modelo;
- Combinação (*Matching*): o modelo recolhido então é comparado a um outro previamente armazenado para que então seja determinado se o traço é ou não do indivíduo analisado.

Figura 3 – Esboço de um sistema de reconhecimento biométrico



Fonte: LABATI et al., (2016).

Para Liu e Silverman (2001), a verificação ou identificação de usuários definem os sistemas de segurança biométricos. Os autores afirmam que a identificação normalmente é um processo mais trabalhoso pelo fato de que é necessário percorrer vários usuários cadastrados em uma base da dados até encontrar ou não uma possível combinação.

Jain, Flynn e Ross (2007) destacam que para que um sistema biométrico seja confiável este deve atender a alguns requisitos:

- Aceitabilidade: os usuários que passarão por sua utilização devem aceitá-la sem objeções;
- Evasão: deve possuir baixa probabilidade de imitação de traços comportamentais através da utilização de ferramentas para copiar características físicas ou emocionais;
- Distintividade: necessita de uma característica única que diferencie um usuário do restante;
- Mensurabilidade: capacidade de obter os traços biométricos do usuário de maneira adequada, sem causar nenhum distúrbio;
- Performance: habilidade de adquirir as informações de maneira rápida e eficaz;
- Permanência: a avaliação das características biométricas de um usuário não deve apresentar alta taxa de variação ao longo de um determinado período;
- Universalidade: as características analisadas devem estar presentes em qualquer indivíduo.

2.2.2 Métricas avaliativas

Stylios et al. (2021) apresenta algumas métricas básicas para a avaliação da performance de um sistema de autenticação biométrico. São eles:

- Aceitação Verdadeira - *True Acceptance* (TA): representa o número de padrões genuínos que são classificados corretamente como genuínos;
- Rejeição Verdadeira - *True Reject* (TR): representa o número de padrões não genuínos que são classificados corretamente como não genuínos;
- Aceitação Falsa - *False Acceptance* (FA): representa o número de padrões não genuínos que são classificados incorretamente como genuínos;
- Rejeição Falsa - False Reject (FR): representa o número de padrões genuínos que são classificados incorretamente como não genuínos;

Taxa de Aceitação Verdadeira – *True Acceptance Rate* (TAR): trata-se da probabilidade de um padrão ser classificado como genuíno corretamente conforme observado na Equação 1:

$$TAR = \frac{TA}{TA+FR} \quad (1)$$

Taxa de Aceitação Falsa – *False Acceptance Rate* (FAR): representa a probabilidade de classificação de um padrão como genuíno incorretamente conforme observado na Equação 2:

$$FAR = \frac{FA}{FA+TR} \quad (2)$$

Taxa de Rejeição Falsa – *False Rejection Rate* (FRR): descreve a probabilidade de um padrão ser classificado como não genuíno incorretamente conforme observado na Equação 3:

$$FRR = \frac{FR}{FR+TA} \quad (3)$$

Acurácia: é o conceito que representa a probabilidade de classificação correta de um padrão no modelo utilizado conforme observado na Equação 4:

$$Acurácia = \frac{TA+TR}{TA+TR+FA+FR} \quad (4)$$

2.3 Reconhecimento facial

Para Kremic, Subasi e Hakdarevic (2012), o reconhecimento facial tem como base a verificação de dados de entrada e geralmente faz parte de um sistema biométrico. Os autores ainda acrescentam que o conceito artificial do reconhecimento de faces está diretamente ligado à disciplina de visão biológica (estudo dos sistemas e processos envolvidos na percepção visual de humanos e animais), devendo ser considerado como um complemento desta.

O contexto histórico dos estudos relacionados ao reconhecimento facial inicia aproximadamente nos anos de 1950 na área de psicologia e se expandem em 1960 com o surgimento de bibliografia na esfera das engenharias, porém os estudos relacionados ao reconhecimento facial automático e aplicado a máquinas iniciam-se efetivamente nos anos de 1970 (ZHAO et al., 2003). Nos anos de 1990 houve um aumento nos estudos relacionados às tecnologias de reconhecimento facial motivados pela grande evolução de *hardware* e ampliação da necessidade de desenvolvimento de aplicações relacionadas à segurança (Taskiran, Kahraman e Erdem, 2020).

De acordo com Taskiran, Kahraman e Erdem (2020), o reconhecimento facial pode ser abordado como um problema de identificação, onde a nova face analisada é comparada com todas as outras faces previamente registradas em uma base de dados gerando um resultado e uma decisão, ou também como um problema de verificação, onde a identidade é confirmada ou rejeitada baseado na comparação da face em análise com outra face reivindicada do banco de dados.

O reconhecimento facial caracteriza-se por ser um método não intrusivo e potencialmente a maneira mais conhecida utilizada pelos humanos para reconhecer

um indivíduo. Além disso, este método baseia-se em dois principais procedimentos para aplicar a identificação: a localização e feição de traços como boca, nariz, olhos, por exemplo, e a observação geral da imagem do rosto como uma conjunção de um número de rostos canônicos. Levando estes conceitos para a aplicação prática, para que o reconhecimento facial possa funcionar de maneira adequada este deve detectar automaticamente se há um rosto na imagem avaliada, localizar este rosto caso haja um e identificá-lo independentemente da posição de captura do mesmo (JAIN, ROSS e PRABHAKAR, 2004).

Ismail e Sabri (2010), enfatizam que apesar da evolução tecnológica nos últimos anos terem facilitado a aplicação das tecnologias de reconhecimento facial, esta técnica ainda apresenta algumas dificuldades. Para os autores, o reconhecimento facial ainda é de difícil implementação, pois os rostos apresentam diversas variações de pose, formatos, tamanhos e texturas que podem ser grandes complicadores no momento da detecção. Eles listam 6 tipos de problemas que podem dificultar o processo:

- Pose: a posição do rosto pode apresentar muitas variações;
- Presença de componentes estruturais: itens como óculos, máscaras e barbas com formatos e cores diferentes;
- Expressão facial: expressões faciais alteradas;
- Oclusão: dependendo da situação de captura da face, esta pode ser obstruída por outra pessoa ou objeto;
- Orientação da imagem: variação no eixo óptico da câmera;
- Condição da imagem: a imagem capturada pode apresentar uma qualidade baixa dependo da câmera e condições de luz no local.

Zhao et al. (2003) reitera que o grande desafio e interesse pelo estudo do reconhecimento facial resultou em uma variedade de pesquisadores com diferentes tipos de conhecimento e muitos métodos diferentes propostos para o uso desta tecnologia. Desta forma, a ampla e heterogênea literatura da área sucedeu em sistemas baseados em diferentes princípios e técnicas que tornam complexa a sua classificação. Apesar desta variedade, os autores categorizam os métodos para reconhecimento facial em 3 tipos:

- Métodos de combinação holísticos: baseia-se na aplicação de toda a face analisada como entrada para o sistema de reconhecimento facial. Neste cenário, as *eigenpictures* são uma das representações mais conhecidas da região facial;
- Métodos de combinação baseados em recursos: atributos do rosto como olhos, nariz, boca, por exemplo, são extraídos e posteriormente suas localizações geométricas e estatísticas são analisadas em classificadores específicos.
- Métodos híbridos: são métodos que combinam as duas opções anteriores e se assemelham muito a forma natural utilizada pelos humanos para aplicar o reconhecimento.

2.3.1 Classificadores

Para redução do custo computacional em sistemas biométricos são aplicados classificadores que dividem as características biométricas em classes para que no momento de aplicar as combinações o processamento seja aplicado somente em amostras da mesma classe (LABATI et al., 2016).

2.3.1.1 Cascata de classificadores

Viola e Jones (2001) propõem um novo método de aplicação de classificadores que apresentou um rendimento mais eficiente se comparado aos melhores sistemas disponíveis anteriormente. O método proposto pelos autores, tem como base a associação de diversos classificadores mais complexos organizados em forma de uma cascata de modo que em cada etapa de aplicação dos classificadores, somente as áreas importantes da imagem fossem levadas em consideração, descartando assim as áreas onde o objeto de interesse não aparece.

2.3.1.2 Eigenfaces

Fujikawa (2016) afirma que os métodos de classificação baseados na correlação normalmente apresentam um custo computacional bastante alto e por conta disto a redução do volume do conjunto de dados é essencial para uma melhor performance. Neste contexto, Bakshi e Prabhu (2017) reiteram que o algoritmo PCA (*Principal Component Analysis*) para extração de características aumenta a eficiência dos sistemas reduzindo a dimensão dos dados e a redundância sem que muitas informações do dado original sejam perdidas.

Segundo Fujikawa (2016), a aplicação do PCA no reconhecimento de faces pode ser traduzida como *eigenface*, que se trata de uma representação linear da imagem dos rostos analisados de maneira que estes possam ser apresentados em baixa dimensão.

O método conhecido como Eigenfaces trata de projetar a imagem capturada em um espaço dimensional menor, conhecido através da utilização das imagens presentes no conjunto de dados de treinamento, para posteriormente compará-la com as faces cadastradas na base de dados (Taskiran, Kahraman e Erdem, 2020).

Para Diniz et al. (2012), o método *Eigenfaces* pode ser caracterizado pela localização de detalhes únicos em uma face que possibilitem a diferenciação de um rosto para outro. Os autores acrescentam que estes detalhes estão presentes na variação de valores encontrada nos pixels de cada imagem de um conjunto de dados.

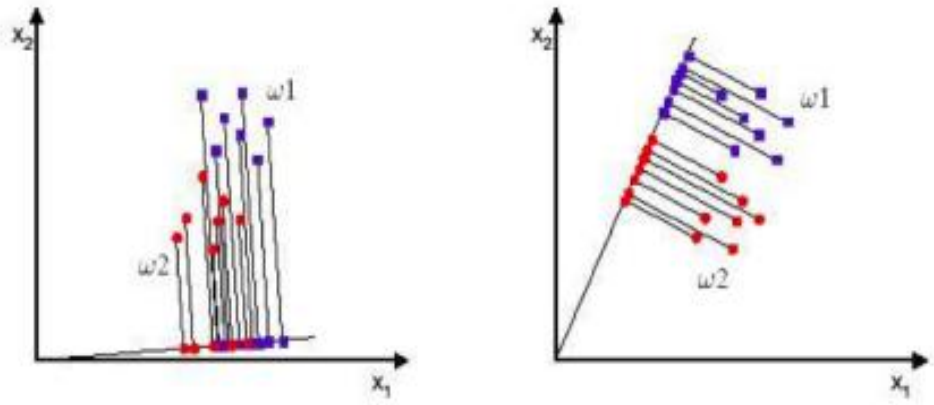
2.3.1.3 Fisherface

De acordo com Fujikawa (2016), a técnica de *Fisherfaces* tem o objetivo de aumentar a dispersão entre as classes, tendo como principal diferença em relação ao *Eigenfaces* a característica de reduzir a dispersão dentro de uma mesma classe, o que diminui as chances de geração de resultados não desejados no momento de

reconhecer os padrões. Um exemplo do funcionamento da técnica é descrito a seguir e pode ser observado na Figura 4:

> Para entender o funcionamento do Fisherface, considere duas classes distintas em um ambiente 2D. Suponha que um conjunto de amostras igual a $x^1, x^2, x^3 \ldots, x^n$ distribuídas entre duas classes, sendo a classe ω1 com N1 amostras e a classe ω2 com N2 amostras. Assim o objetivo é obter uma escalar y onde as amostras x são projetadas em uma reta que maximize a separabilidade dos escalares como pode ser observado na Figura (CARNEIRO, 2012, p.32).

Figura 4 – Reta com a indicação das posições de maior separabilidade dos conjuntos



Fonte: Carneiro, (2012).

Neste capítulo foi construída a abordagem teórica que será utilizada como base durante o desenvolvimento deste trabalho. Foram apresentados conceitos relacionados aos sistemas de segurança, especialmente relacionados ao controle de acesso, bem como os princípios da biometria e como esta se aplica no campo tecnológico através dos sistemas biométricos. Além disso, foram abordadas as métricas de avaliação que permitem analisar e gerar estatísticas acerca dos resultados de um sistema biométrico. Por fim, a pesquisa bibliográfica também foi direcionada para a tecnologia de reconhecimento facial tratando de características mais específicas como os classificadores e algumas técnicas utilizadas.

3 TRABALHOS RELACIONADOS

Serão apresentados neste capítulo trabalhos relacionados, nos quais as tecnologias que empregam técnicas biométricas foram aplicadas como ferramenta para atingir os objetivos propostos. Além disso, serão destacadas as diferenças e pontos em comum entre estes trabalhos e a proposta atual.

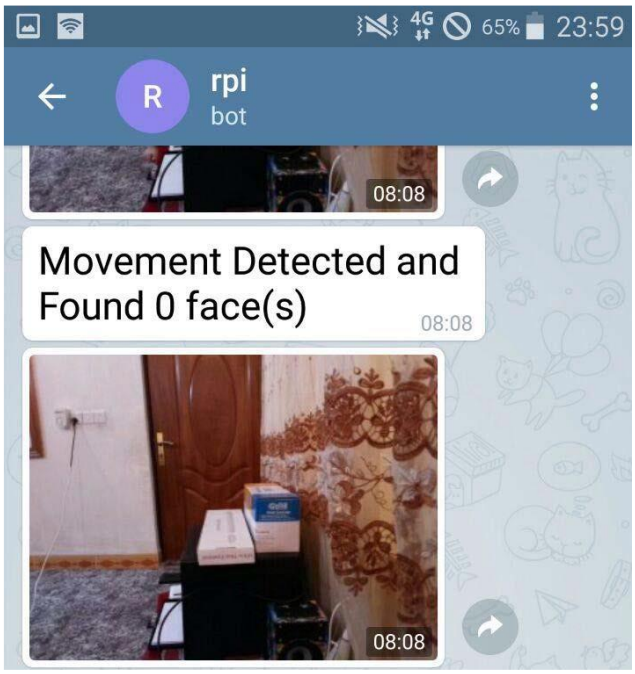
3.1 Reconhecimento Facial para Segurança com Raspberry PI

Aydin e Othman (2017), desenvolveram uma nova proposta de aplicação para segurança baseando-se em conceitos como Internet das Coisas e visão computacional. O objetivo desta solução é eliminar a necessidade de ter uma pessoa detectando possíveis problemas analisando imagens capturadas por uma câmera. Desta forma, a solução proposta visa combinar o reconhecimento facial com dispositivos como sensores e câmeras integrados e conectados a uma rede para que em caso de detecção de intrusão o usuário seja notificado automaticamente.

Para desenvolver o sistema proposto, os autores utilizaram um Raspberry PI 3 em conjunto com uma PICAMERA. A captura da câmera é acionada caso o sensor PIR (*Passive infrared sensor*) detecte qualquer tipo de movimento no local onde está instalado. Após isto, a detecção facial é aplicada utilizando o algoritmo de Haar

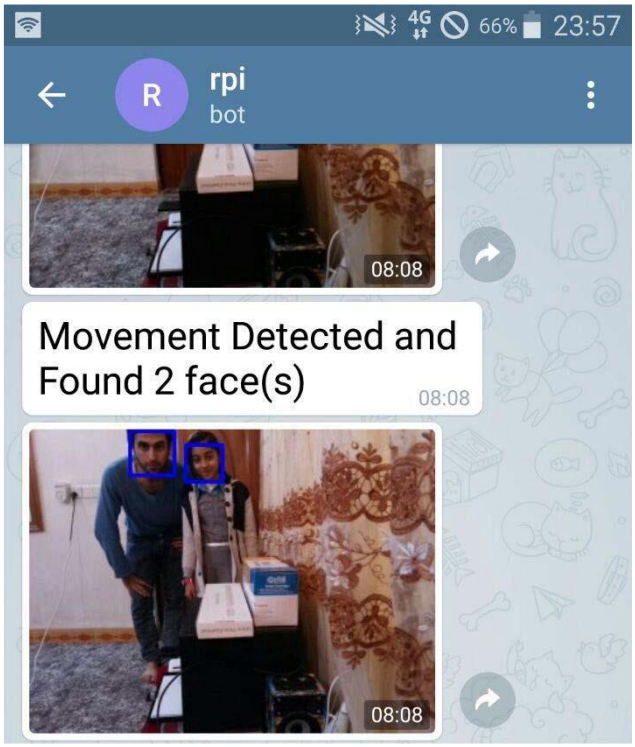
Cascade e então notificações e imagens capturadas são enviadas para o usuário através do aplicativo Telegram, conforme pode-se observar na Figura 5 e Figura 6.

Figura 5 – Tela de notificação do sistema com nenhuma face encontrada



Fonte: AYDIN e OTHMAN, (2017).

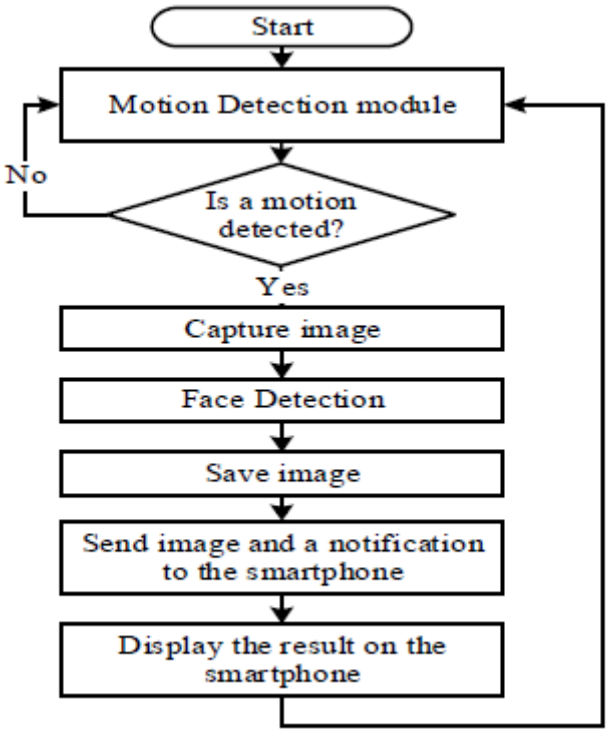
Figura 6 – Tela de notificação do sistema com duas faces encontradas



Fonte: AYDIN e OTHMAN, (2017).

A Figura 7 apresenta o fluxograma do sistema proposto que segue as seguintes etapas.

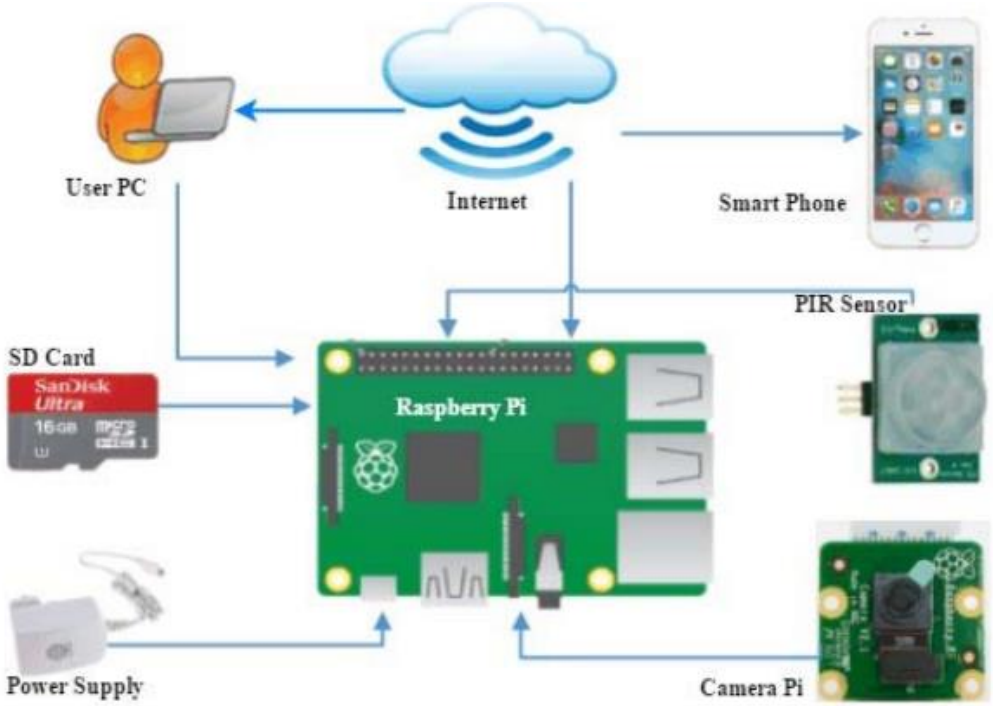
Figura 7 – Fluxograma para o sistema proposto



Fonte: AYDIN e OTHMAN, (2017).

Os autores afirmam que o Raspberry PI se trata de um pequeno controlador com quatro módulos de conexão USB e possibilidade de conexão *bluetooth* ou WiFi. Para o seu projeto ainda foram incorporadas ao dispositivo, uma PICAMERA que possui a função de capturar as imagens e um sensor PIR responsável por detectar o movimento dos objetos ao seu redor. O design projetado para o sistema pode ser observado na Figura 8.

Figura 8 – Design do sistema de reconhecimento facial utilizando Raspberry PI



Fonte: AYDIN e OTHMAN, (2017).

É possível observar que o sistema sugerido pelos autores se destaca positivamente no sentido de apresentar novas possibilidades para a aplicação de sistemas de segurança em casas ou até mesmo em ambientes públicos. Além disso, as ferramentas utilizadas não apresentam um custo elevado, abrindo assim a possibilidade de utilização desta tecnologia por ainda mais pessoas ou empresas interessadas.

3.2 FaceNet

O sistema FaceNet é uma iniciativa criada em 2015 por pesquisadores vinculados a Google que atingiram resultados excelentes utilizando conjuntos de dados conhecidos como LFW (*Labled Faces in the Wild*) e Youtube Faces DB se comparado a performance atingida por outros sistemas citados como referência em seu trabalho. O LFW se trata de um conjunto de dados acadêmico famoso para verificação de faces e tem como característica a análise de pares de imagens para a obtenção dos resultados, por outro lado o Youtube Faces DB é caracterizado por

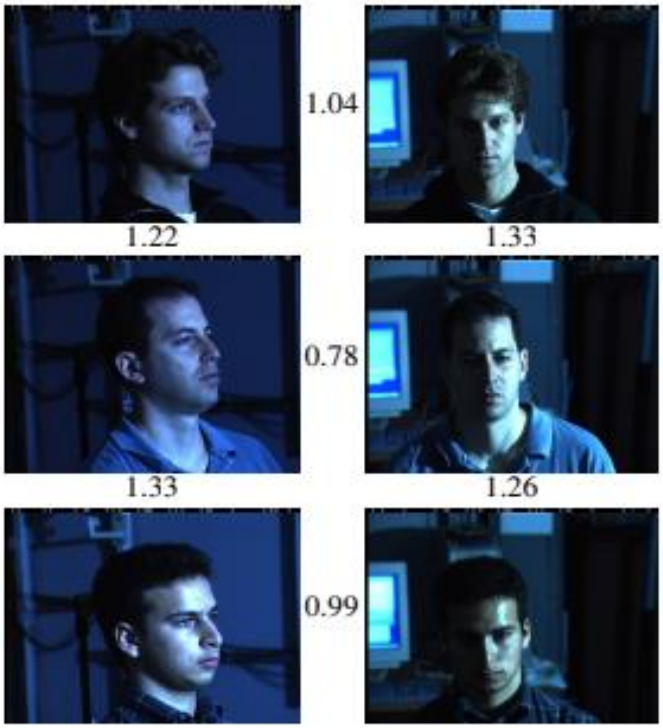
ser um conjunto de dados para análise de pares de vídeos (SCHROFF, KALENICHENKO e PHILBIN, 2015).

De acordo com Schroff, Kalenichenko e Philbin (2015), o sistema baseia-se no conceito de espaço euclidiano onde as distâncias calculadas de cada rosto são aprendidas por uma rede neural convolucional e geram um mapeamento que serve como representação de uma medida para avaliar a semelhança dos rostos analisados. Após obter o mapeamento dos espaços, tarefas como o reconhecimento, verificação e agrupamento se tornam mais simples de serem aplicadas. Os autores ainda acrescentam que o treinamento da rede baseado nas distâncias quadradas dos espaços incorporados nas imagens representa diretamente a semelhança dos rostos, sendo que as faces das mesmas pessoas apresentam distâncias menores enquanto as faces de pessoas distintas resultam em um maior espaçamento.

O sistema possui a capacidade de realizar a verificação de pessoas (compara duas imagens e define se são a mesma pessoa), reconhecimento (possibilita avaliar quem é a pessoa na imagem obtida) e agrupamento (consegue encontrar pessoas em comum dadas algumas imagens de rostos).

Na Figura 9 podem ser observadas as distâncias calculadas pelo FaceNet em comparações de imagens das mesmas pessoas e entre pessoas distintas em posições e condições de iluminação variadas. A métrica de avaliação do sistema define que quanto mais próximo ao 0.0 maior a semelhança e quanto mais aproximado de 4.0 maior a divergência de traços. A Figura 10 apresentada imagens classificadas incorretamente pelo FaceNet utilizando o conjunto de dados LFW.

Figura 9 – Análise de imagens com variação de poses e iluminação



Fonte: SCHROFF, KALENICHENKO e PHILBIN, (2015).

Figura 10 – Imagens classificadas incorretamente no conjunto de dados LFW

Fonte: SCHROFF, KALENICHENKO e PHILBIN, (2015).

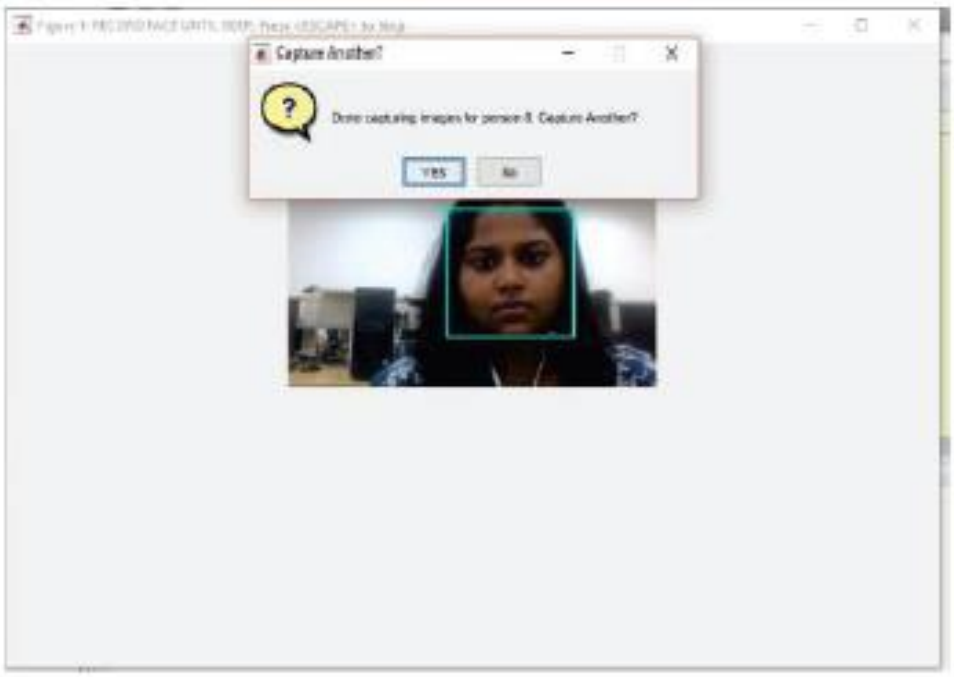
Levando em consideração as taxas de acurácia reportadas pelos pesquisadores, no conjunto de dados LFW o sistema pode atingir um novo recorde de acurácia de 99.63% e no conjunto de dados Youtube Faces DB de 95.12% (diminuindo em 30% as taxas de erro em relação às melhores publicações até o momento). É possível afirmar que o modelo utilizado apresenta um avanço considerável e uma grande relevância no contexto acadêmico e prático do estudo de reconhecimento facial.

3.3 Reconhecimento facial utilizando o algoritmo PCA

Bakshi e Prabhu (2017) destacam em seu trabalho que a demanda para sistemas de segurança, especialmente envolvendo a identificação de pessoas, tem aumentado muito nos últimos anos. Neste sentido, os autores desenvolveram uma aplicação de reconhecimento facial atrelada a uma trava de segurança utilizando um dos algoritmos mais conhecidos no ramo acadêmico, o PCA (*Principle Component Analysis*), que tem a função de extrair características e padrões das imagens captadas.

A captura de vídeo do sistema proposto é efetuada por um módulo de detecção de movimento em conjunto com uma *web-cam*. Em caso de identificação de alguma movimentação, o módulo de detecção facial é então acionado e aplica a busca por padrões e características de uma face na imagem obtida, conforme Figura 11. Tendo sido encontrado um rosto, o próximo passo é a extração das faces encontradas na imagem, através de coordenadas, e a conversão para um formato acessível pelo banco de dados. Na etapa final, o rosto detectado é comparado com todos os outros cadastrados na base de dados, enviando um sinal para o microcontrolador e exibindo o resultado em tela, como apresentado na Figura 12, caso este seja reconhecido. As faces detectadas passam por um processo de validação onde o usuário confirma se estas correspondem realmente à pessoa indicada pelo sistema, como pode ser observado na Figura 13.

Figura 11 – Captura inicial do vídeo

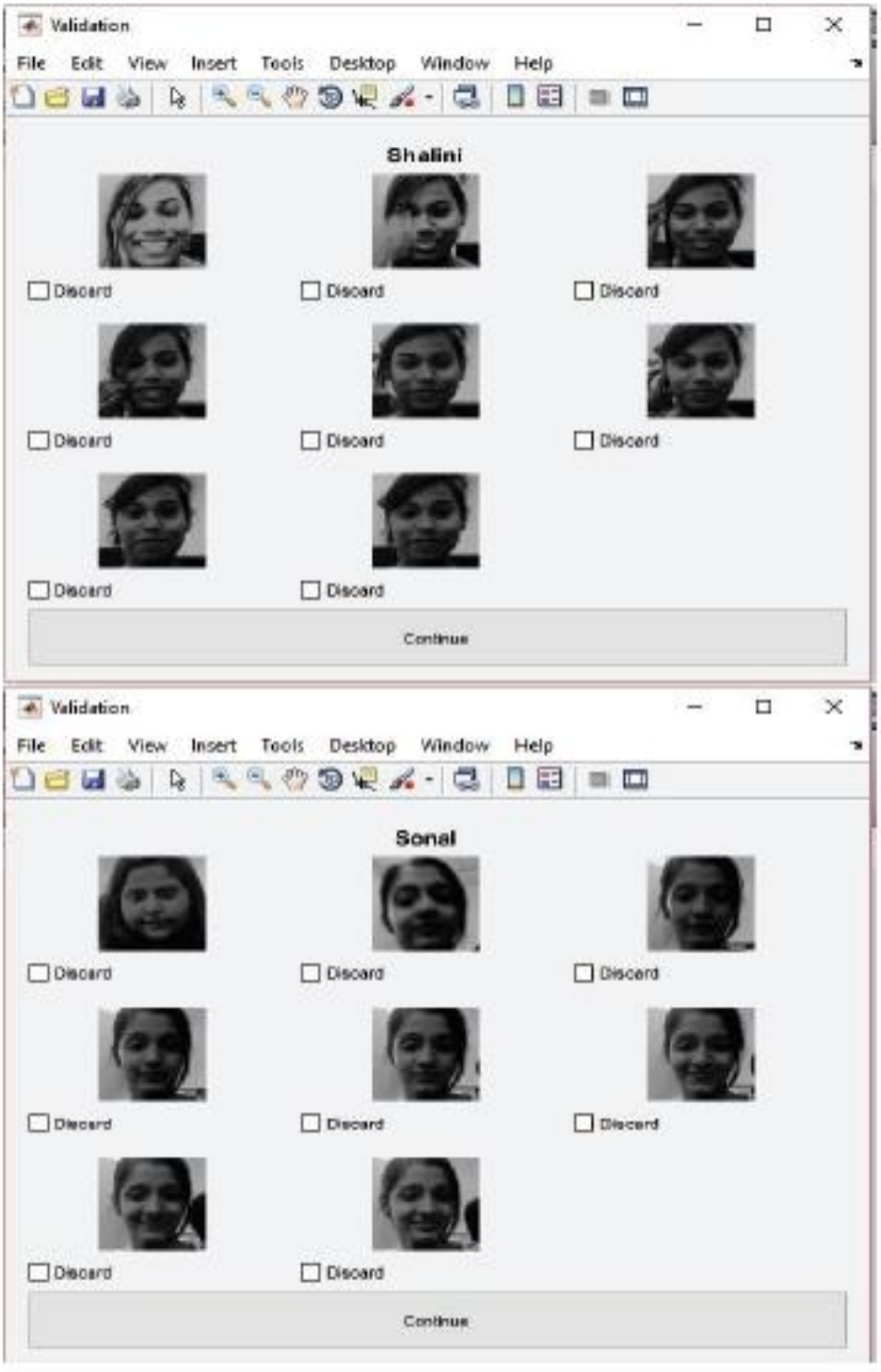


Fonte: BAKSHI e PRABHU, (2017).

Figura 12 – Resultado apresentado em tela

Fonte: BAKSHI e PRABHU, (2017).

Figura 13 – Etapa de validação das faces



Fonte: BAKSHI e PRABHU, (2017).

Os módulos de detecção de movimento, reconhecimento e detecção facial foram desenvolvidos utilizando uma plataforma chamada MATLAB. Este sistema integra um ambiente *desktop* focado em análises iterativas que conta com uma linguagem de programação capaz de expressar matrizes e vetores matemáticos de forma direta (MATHWORKS). Já o microcontrolador se trata de um *Arduino Uno*, uma plataforma para projetos interativos de simples utilização *open-source* com capacidade de interpretar sinais de sensores e controlar estes sinais através de código que também pode ser inserido no dispositivo (ARDUINO).

É possível afirmar, conforme a conclusão dos autores, que as tecnologias utilizadas servem para serem aplicadas em um sistema real de reconhecimento facial, porém, preferencialmente em um ambiente controlado com poucas variações de luz e posicionamento das faces no momento da captura das imagens, visto que a taxa de acurácia do sistema apresentado está diretamente relacionada com as condições do local.

3.4 Estudo comparativo dos algoritmos de reconhecimento facial da biblioteca OpenCV

Galimberti (2018) afirma que a ascensão da utilização de técnicas de biometria facial em sistemas de controle de acesso em conjunto com a escassez de estudos que comparam a eficiência dos diferentes algoritmos de reconhecimento facial motivou a elaboração deste estudo.

Neste contexto, foi desenvolvido um protótipo de um sistema de controle de acesso em uma empresa de tecnologia com a finalidade de comparar o desempenho dos diferentes algoritmos presentes na biblioteca de visão computacional *OpenCV: Eigefaces, Fisherfaces* e LBPH.

O protótipo desenvolvido conta com a utilização de um *Raspberry Pi 3 Model* B em conjunto com uma câmera de resolução 8MP e um *speaker*. O sistema instalado no *Raspberry Pi* é responsável por executar o processo de detecção facial respondendo ao usuário com um áudio informando se este possui ou não

autorização. Também está presente nesta ferramenta um simulador para o sinal de abertura de uma porta que é representado por um *Light Emitter Diode* (LED) que está integrado *Raspberry Pi.*

Além disso, foi implementada uma aplicação que, após receber o sinal de que uma nova face foi detectada, executa a tarefa de reconhecimento facial e retorna o resultado. Também estão presentes na ferramenta telas que possibilitam o gerenciamento dos usuários e imagens que passarão pelos processos já mencionados. Esta solução foi instalada em um servidor Linux e a comunicação com o *Raspberry Pi* ocorreu via *webservice*.

O autor conclui que o algoritmo *Fisherfaces* se sobressaiu em relação aos outros tanto no aspecto das taxas de reconhecimentos quanto na agilidade para finalização de todo o processo. Vale destacar que este resultado pode variar de acordo com que o local de posicionamento da câmera é alterado.

É importante mencionar que o presente estudo tem relação direta com o trabalho do autor, visto que ambos são aplicados na mesma empresa. O intuito é dar continuidade ao trabalho, alterando o local onde os reconhecimentos são realizados para o ambiente definitivo selecionado pela companhia e avaliando a experiência dos colaboradores que estarão sujeitos ao processo de reconhecimento facial.

3.5 Relação com o trabalho desenvolvido

A partir da análise dos trabalhos relacionados, é possível destacar que o campo da visão computacional, especialmente o reconhecimento facial, é uma área com bastante espaço para crescimento. Apesar disto, os autores mencionam que ainda existem muitos desafios a serem enfrentados para que a utilização desta tecnologia se torne viável em ambientes não controlados. Questões como luminosidade, variações na posição das faces e expressões faciais se apresentam como grandes vilões neste processo.

A constante necessidade de modernização do mercado da segurança abre um amplo espaço para o uso destas tecnologias, portanto, a necessidade de exploração do tema por parte da comunidade acadêmica será continuamente necessária para que novas alternativas que viabilizem o uso do reconhecimento facial.

Levando em consideração os trabalhos relacionados citados, o presente trabalho está sendo elaborado com o intuito de desenvolver uma ferramenta que possa contribuir com este processo de aprimoramento do uso da tecnologia de reconhecimento facial.

4 MÉTODOS E MATERIAIS

Este capítulo apresenta a metodologia e tecnologias empregadas no desenvolvimento deste trabalho, detalhando a implementação e funcionalidades da ferramenta de reconhecimento facial proposta.

4.1 Classificação da pesquisa

No âmbito dos procedimentos metodológicos, esta pesquisa classifica-se como bibliográfica e documental na etapa de fundamentação, onde o embasamento teórico é construído para auxiliar na compreensão do conteúdo apresentado no trabalho. Prodanov e Freitas (2013) destacam que a pesquisa bibliográfica tem o objetivo de minimizar eventuais incongruências corroborando a autenticidade das informações apresentadas através da coleta de materiais publicados. Lakatos e Marconi (2010) acrescentam que a pesquisa bibliográfica amplia as perspectivas de um mesmo tema a partir das novas conclusões formadas por outros autores.

Em relação aos objetivos, o fato de o trabalho envolver o desenvolvimento de um sistema de reconhecimento facial, caracteriza-o também como uma pesquisa experimental. Para Prodanov e Freitas (2013) trata da exposição dos objetos de estudo para que estes sofram influência de variáveis em ambientes controlados pelo investigador e, a partir disto, observar as possíveis alterações estabelecidas como resultado.

A abordagem exploratória também está presente nesta pesquisa pelo fato desta investigar de que maneira a aplicação de uma tecnologia de reconhecimento facial pode auxiliar na segurança de um ambiente. Para Lakatos e Marconi (2010) este tipo de abordagem está relacionado com a observação empírica das situações que envolvem o objeto de estudo com o objetivo de formular um problema que auxilia na elaboração de hipóteses, expansão de conhecimento do autor sobre o tema em estudo e no desenvolvimento de um possível trabalho futuro que contenha mais precisão.

O tipo de pesquisa do presente trabalho pode ser classificado como qualitativo e quantitativo. Qualitativo no sentido de interpretar os resultados fornecidos pelo sistema de reconhecimento facial e descrevê-los de maneira a compreender se estes são eficientes em uma aplicação real. Quantitativo com relação à análise dos números gerados pelos algoritmos empregados para verificar se a aplicação foi eficaz ou não no que se propôs a atender. Para Gerhardt e Silveira (2009), a pesquisa qualitativa tem o foco no esclarecimento dos fenômenos sociais e as relações entre eles. Desta forma, a representatividade numérica dos resultados não é utilizada, obtendo-se o conhecimento através de informações aprofundadas e ilustrativas. Para Sampieri, Collado e Lucio (2013), o pesquisador que aplica uma visão quantitativa de pesquisa necessita coletar dados específicos para testar as suas hipóteses, aplicando métodos matemáticos à estas informações para que os resultados desejados possam ser comprovados.

4.1 Tecnologias

As tecnologias apresentadas nas sessões a seguir estarão presentes no desenvolvimento deste trabalho e são fundamentais para que os objetivos propostos sejam atingidos.

4.1.1 Java

O *Java* é uma linguagem de programação orientada a objetos lançada em 1995 com suporte para uma grande quantidade de plataformas computacionais (JAVA, 2020).

No trabalho proposto o *Java* será utilizado para o desenvolvimento da aplicação que será disponibilizada aos gestores para que estes obtenham as informações coletadas pelo sistema de reconhecimento facial e possam fazer o gerenciamento e acompanhamento das faces que estão sendo comparadas. Nesta aplicação, os usuários terão a possibilidade de visualização do histórico de comparações das faces capturadas bem como a permissão para excluir ou adicionar novas faces à base de dados utilizada para a comparação.

4.1.2 Banco de dados

Os bancos de dados em aplicações servem como uma ferramenta auxiliar para realizar o armazenamento dos dados utilizados. Para o desenvolvimento deste trabalho será utilizado o MariaDB que se trata de um dos servidores mais populares do mundo.

A escolha da base de dados se deu pelo fato de sua agilidade, escalabilidade e robustez, características estas que são fundamentais em sistemas de grande porte como é o caso do *Strategic Adviser*.

4.1.3 Python

A linguagem de programação *Python*, disponível desde 1992, é reconhecida por ser uma linguagem de alto nível, orientada a objetos e com uma sintaxe simples para facilitar a manutenção de código. Além disso, algumas das principais

características do *Python* é sua capacidade de aumentar a produtividade dos desenvolvedores e a grande quantidade de bibliotecas que possibilitam a utilização de recursos de diversas áreas diferentes como ciência de dados e inteligência artificial (PYTHON, 2020).

A utilização do *Python* neste trabalho ocorrerá em conjunto com a biblioteca *OpenCV-Python* que é uma adaptação da biblioteca original desenvolvida em *C++.* A escolha desta linguagem foi baseada na possibilidade de ganho de produtividade e manutenção de código, visto que uma de suas características é a possibilidade de implementação de diversas tarefas em um código enxuto. Além disso, a utilização do *Python,* tem sido uma tendência cada vez maior na área de visão computacional que será contemplada nesta pesquisa.

4.1.4 OpenCV

O *OpenCV* é uma biblioteca gratuita desenvolvida em 2000 pela Intel, focada em visão computacional e *machine learning* que conta com a presença de milhares algoritmos abordados dentro destas áreas de conhecimento. O objetivo no desenvolvimento desta biblioteca está em prover um ambiente com uma infraestrutura comum para agilizar a utilização da percepção de máquina em aplicações comerciais (OPENCV, 2020).

Neste trabalho, a biblioteca será utilizada combinada à linguagem de programação *Python* para a aplicação dos algoritmos de visão computacional necessários durante as etapas do reconhecimento facial. Alguns dos algoritmos presentes nesta biblioteca são o *Eigenfaces* e o *Fisherfaces*, ambos foram abordados na etapa do referencial teórico da pesquisa.

4.1.5 Strategic Adviser

O sistema de gestão corporativa *Strategic Adviser* da empresa *Interact Solutions* conta com uma suíte de aplicações que tem como finalidade proporcionar ferramentas que auxiliam na estratégia de gestão das organizações (INTERACT, 2021). A solução proposta neste trabalho será integrada a este conjunto de ferramentas, agregando mais uma funcionalidade ao sistema.

4.2 Desenvolvimento

Com o propósito de atingir os objetivos especificados na atual proposta de trabalho, foi desenvolvida uma aplicação de reconhecimento facial para a plataforma *web*, que faz parte de uma suíte de aplicações do *software Strategic Adviser*, da empresa *Interact Solutions*. Esta ferramenta auxilia no controle de acesso às dependências da empresa, indicando se as pessoas têm ou não permissão de acesso através da porta principal.

Uma câmera IP com resolução *HD* instalada ao lado da porta de entrada da empresa realiza a captura das imagens assim que algum rosto for identificado. Estas imagens são enviadas, via rede, para um servidor interno que as armazena, para que estas sejam utilizadas em etapas subsequentes do processo.

No momento em que for identificada a captura de uma nova face, o algoritmo de reconhecimento facial é acionado, coletando a imagem capturada e aplicando uma comparação com abordagem 1:N, o que significa que a nova face será comparada com cada uma das N faces cadastradas no modelo de pessoas autorizadas.

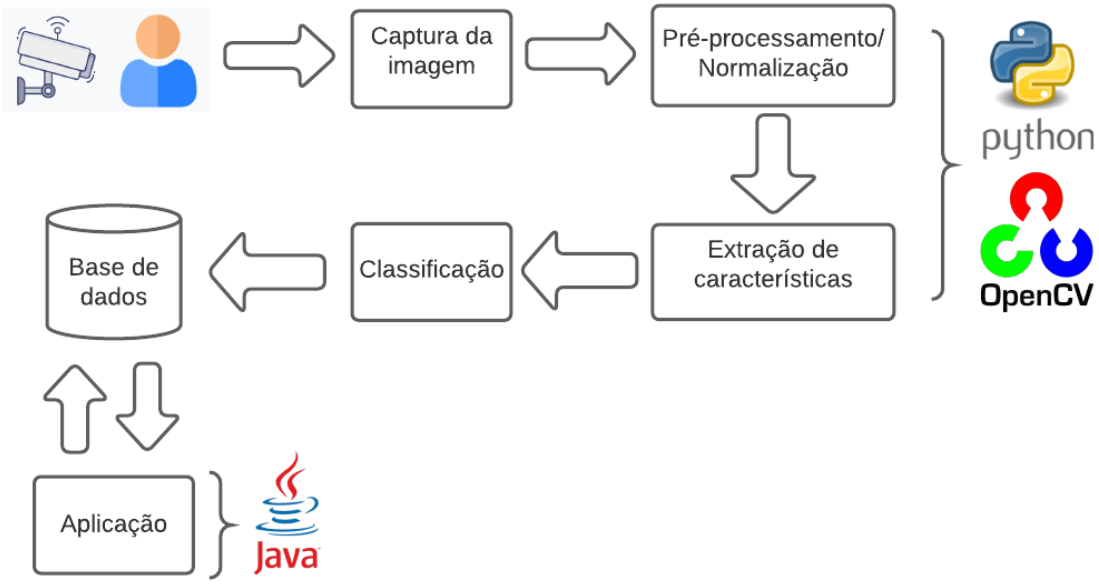
O aplicativo conta também com uma interface para administração da ferramenta por parte dos gestores. Neste ambiente fica registrado todo o histórico de novas faces capturadas e as porcentagens de assertividade após a comparação

com as imagens já cadastradas no modelo. Além disso, é possível, através desta interface, excluir ou adicionar imagens no conjunto de dados.

4.2.1 Arquitetura

Na Figura 14 pode ser observada a arquitetura que representa o fluxo de funcionamento do sistema proposto neste trabalho.

Figura 14 – Arquitetura do sistema



Fonte: Do autor (2020).

O fluxo de desempenho do sistema inicia-se na etapa de captura das imagens, onde os colaboradores ou visitantes deverão parar em frente a uma câmera de segurança localizada ao lado da porta de entrada principal da empresa para que sua face seja detectada e uma foto seja obtida. Nesta fase o sistema aplica algoritmos presentes na biblioteca OpenCV capazes de extrair as faces localizadas em vídeo. É utilizada uma câmera com resolução *HD* para que se tenha uma melhor qualidade na obtenção das imagens, facilitando assim o trabalho do reconhecimento facial que será aplicado nos próximos passos.

Após a aquisição de uma nova face, entra em ação a etapa de pré-processamento ou normalização da imagem obtida. Este passo é importante, pois visa aplicar tratamentos de maneira a facilitar a execução do processo de reconhecimento facial. Em todas as capturas realizadas são aplicadas correções para que assim o mesmo padrão de imagem possa ser passado adiante no processo.

Ao finalizar a normalização, a imagem corrigida é repassada para que se inicie o estágio onde as características da face são extraídas. Neste ponto, é importante ressaltar que a imagem deve ser convertida de alguma maneira que possa ser representada numericamente para que seja possível encontrar os padrões durante a etapa de classificação. Desta forma, a representação utilizada para imagens é de uma matriz, onde cada pixel da imagem pode ser entendido como uma posição deste *array*.

Na etapa final do processo, um classificador de padrões é aplicado, utilizando as características obtidas na etapa anterior para comparar a nova face com as faces registradas no modelo de dados e definir se esta é conhecida ou não. É importante destacar que cada nova face obtida será comparada com todas as faces registradas no modelo. Em princípio, a abordagem de comparação utilizada não representa um problema, visto que não deverá ser mantida uma quantidade de faces cadastradas grande o suficiente a ponto de aumentar o custo computacional significativamente.

4.2.2 Requisitos de Software

A seguir serão apresentados os quadros que contém o levantamento de requisitos funcionais e não funcionais realizado para determinar as funcionalidades da aplicação desenvolvida.

Os requisitos funcionais (Quadro 1) são caracterizados pelas ações e serviços oferecidos pelo sistema para os usuários. Já os requisitos não funcionais (Quadro 2) estão ligados às tecnologias e infraestrutura utilizados durante o processo de desenvolvimento.

Quadro 1 – Requisitos funcionais (Continua)

Requisito	Descrição	Prioridade
RF01 – Possibilitar cadastro de novas faces	A aplicação deverá permitir o cadastro de novas faces que serão utilizadas para a comparação realizada pelo algoritmo de reconhecimento facial.	Obrigatório
RF02 – Possibilitar exclusão de faces	A aplicação deve permitir a exclusão de faces existentes no modelo.	Obrigatório
RF03 – Detectar faces	A aplicação deve detectar faces no vídeo da câmera e capturar imagens para que fiquem acessíveis ao algoritmo de reconhecimento facial.	Obrigatório
RF04 – Aplicar reconhecimento de faces	A aplicação deve obter as imagens capturadas pela câmera e compará-las com as imagens existentes no modelo para definir se reconhece ou não o usuário.	Obrigatório
RF05 – Calcular assertividade dos reconhecimentos	O aplicativo deve gravar e apresentar em tela a porcentagem de assertividade dos reconhecimentos.	Obrigatório
RF06 – Manter histórico de faces detectadas	Um histórico de faces detectadas deve ser mantido.	Obrigatório
RF06 – Possibilitar exclusão de reconhecimentos	A aplicação deve permitir a exclusão de registros de reconhecimento.	Obrigatório

Quadro 1 – Requisitos funcionais (Conclusão)

RF06 – Identificar ocorrências de pessoas desconhecidas	O aplicativo deve destacar em tela reconhecimentos de pessoas desconhecidas	Obrigatório
RF07 – Exibir estatísticas dos reconhecimentos	O aplicativo deve exibir em tela estatísticas (média e desvio padrão) dos registros de reconhecimento	Obrigatório

Fonte: Do autor, (2021).

Quadro 2 – Requisitos não funcionais (Continua)

Requisito	**Descrição**	**Prioridade**
RNF01 – Linguagem de programação para a interface	Desenvolvimento da interface de administração utilizando a linguagem de programação Java	Obrigatório
RNF02 – Linguagem de programação para a ferramenta de reconhecimento facial	Desenvolvimento da ferramenta de reconhecimento facial utilizando a linguagem de programação Python	Obrigatório
RNF03 – Biblioteca OpenCV	Desenvolvimento da ferramenta de reconhecimento facial utilizando a biblioteca de visão computacional OpenCV	Obrigatório
RNF04 – Armazenamento das informações	Compatibilidade com banco de dados MariaDB para o armazenamento das informações necessárias.	Obrigatório

Quadro 2 – Requisitos não funcionais (Conclusão)

RNF05 –Plataforma de execução	Desenvolvimento da aplicação para a plataforma *web*	Obrigatório
RNF06 –Navegador	Compatibilidade com os navegadores Google Chrome, Firefox, Internet Explorer e Safari	Obrigatório
RNF07 –Sistema Operacional	Compatibilidade com os sistemas operacionais Linux e Windows	Obrigatório

Fonte: Do autor, (2021).

4.2.3 Alimentação do modelo

A alimentação do modelo de faces autorizadas é realizada através de um *script*, que é acionado por meio de uma requisição realizada pelo servidor do software *Strategic Adviser*, assim que o gestor finaliza o cadastro dos usuários autorizados.

Para viabilizar a alimentação do modelo de faces autorizadas, foi implementada uma API *REpresentational State Transfer* – REST, junto ao *script* de treinamento, com tratamento para o método POST. No momento em que o gestor finaliza o cadastro de faces autorizadas, é enviada uma requisição à API contendo um JavaScript Object Notation – JSON. Este JSON carrega o *id* e as imagens inseridas para cada um dos usuários registrados. Ao receber estas informações, a API limpa o diretório de faces autorizadas no servidor e insere os arquivos novos nomeando-os com a informação do *id*.

Conforme pode ser observado na Figura 15, no momento do acionamento do *script* um diretório específico para o armazenamento das imagens de faces autorizadas é acessado e estes arquivos são carregados para objetos em memória. Em seguida, todas as imagens presentes no diretório são percorridas e modificadas

para a escala de cinza, que é um formato de melhor interpretação dentro dos modelos do *OpenCV*. Posteriormente, as imagens e os *ids* dos usuários são armazenados em listas que são passadas como parâmetro para o método *train,* que irá realizar efetivamente o treinamento do modelo. Os dados de treinamento do modelo são gravados em um arquivo YAML para que possam ser acessados durante a etapa de reconhecimento facial.

Figura 15 – Treinamento do modelo

```
training_faces = [f for f in listdir(training_path) if isfile(join(training_path, f))]

training_data, subjects = [], []

for i, arq in enumerate(training_faces):
    image_path = training_path + arq
    image = standardize_image(image_path)
    training_data.append(image)
    subject = arq[3:5]
    subjects.append(int(subject))

subjects = np.asarray(subjects, dtype=np.int32)

#cria, treina e salva o modelo LBPH
lbph_model = cv2.face.LBPHFaceRecognizer_create()
lbph_model.train(training_data, subjects)
lbph_model.save("lbph_trainner.yml")
```

Fonte: Do autor (2021).

4.2.4 Detecção e reconhecimento facial

Esta etapa é responsável por determinar se um usuário está autorizado a acessar as dependências da empresa e está segmentada em dois estágios principais: captura do padrão facial e predição do modelo. As fases mencionadas são detalhadas a seguir.

4.2.5 Captura do padrão facial

Para que as faces dos usuários sejam capturadas, conforme detalhado na Figura x15 é realizado o acesso via rede à câmera de segurança, localizada ao lado

da porta principal da empresa. O acesso é efetuado através do protocolo *Real Time Streaming Protocol* (RTSP), que é ideal para transferências de dados em tempo real.

A localização do padrão facial nos frames capturados pela câmera necessita do carregamento de um classificador em memória. Este classificador é um arquivo *Extensible Markup Language* (XML), disponível no projeto do OpenCV, na plataforma GitHub, que contém as informações referente ao padrão dos objetos que se deseja detectar. Neste caso, foi utilizado o classificador que contém os dados de uma face visualizada de forma frontal.

Com o acesso à câmera estabelecido e o classificador carregado em memória, inicia-se um processo de repetição que percorre os frames recuperados em tempo real. As imagens capturadas são convertidas para escala de cinza e enviadas como parâmetro para o método *detectMultiScale,* que realiza o processo de detecção facial, baseando-se no classificador carregado anteriormente. Ao localizar o padrão, o frame é armazenado em memória e inicia-se um novo processo de repetição, que percorre as coordenadas (x,y) e as medidas de altura e largura das faces encontradas, para que assim seja possível extrair a *Region of Interest* (ROI), que contém o recorte exato do rosto detectado.

4.2.6 Predição do modelo

O processo de predição do modelo, detalhado na Figura 16, é acionado sempre que uma nova face for detectada. A execução é efetuada através do método *predict,* presente no objeto que carrega o modelo treinado a partir do arquivo YAML. mencionado anteriormente. É enviado como parâmetro para o método de predição a face extraída durante o processo de detecção facial, porém, redimensionada para as medidas das imagens presentes no modelo e convertida para escala de cinza.

Ao aplicar a predição são retornados pelo modelo os valores *id,* que se refere ao identificador do usuário reconhecido, e *confidence,* que pode ser compreendido como o cálculo da distância euclidiana entre a face enviada como parâmetro e o

usuário que o modelo identificou, isto é, quanto menor o resultado deste cálculo, maior a similaridade entre os objetos analisados.

Para determinar se uma face foi reconhecida, se faz necessária a definição de um valor limiar máximo para a medida de *confidence* retornada pelo modelo. Caso o valor exceda a medida determinada, o usuário é classificado como não reconhecido pela aplicação. Neste estudo, o valor limiar definido é o *confidence* de menor número dentre a predição de 10 usuários não treinados no modelo utilizado.

Por fim, são coletadas as informações *id*, imagem capturada, *confidence*, indicação de reconhecimento do usuário (0 ou 1), hora e data do momento exato da ocorrência de reconhecimento e inseridos na base de dados utilizada pelo software Strategic Adviser.

Figura 16 – Detecção facial e predição do modelo

```
capture=cv2.VideoCapture('rtsp://mx:[redacted]:554/cam/realmonitor?channel=1&subtype=0')

frontalface=cv2.CascadeClassifier(r'C:\Users\mx\face_recognition\haarcascade_frontalface_default.xml')

threshold=calculate_threshold()

captures_path=r'C:\\Users\\mx\\face_recognition\\captures\\'

i=0

try:
    while(True):
        capture_ok, frame = capture.read()

        if capture_ok:
            frame = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
            frame_resized = cv2.resize(frame, (400,300))
            gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
            faces = frontalface.detectMultiScale(gray, 1.3, 7)

            if len(faces) > 0:
                i+=1
                for (x,y,w,h) in faces:
                    roi = frame[y:y+h, x:x+w]
                    roi = cv2.cvtColor(roi, cv2.COLOR_BGR2RGB)
                    filePath = captures_path + str(i) + ".png"
                    cv2.imwrite(filePath, roi)
                    face = standardize_image(filePath)
                    lbph_recognizer = cv2.face.LBPHFaceRecognizer_create()
                    lbph_recognizer.read("lbph_trainner.yml")
                    _id, confidence = lbph_recognizer.predict(face)
                    isKnown = 0 if confidence > threshold else 1
                    assertiveness = calculate_assertiveness(threshold, confidence)
                    insertData( _id,
                                convertToBinaryData(filePath),
                                assertiveness,
                                isKnown,
                                datetime.now() )

        show_video(frame_resized)

except KeyboardInterrupt:
    capture.release()
```

Fonte: Do autor (2021).

4.3 Aplicação para o gerenciamento das faces

A ferramenta de gerenciamento e acompanhamento das atividades relacionadas ao reconhecimento facial foi implementada na forma de um aplicativo incorporado ao software *Strategic Adviser* da empresa *Interact Solutions*.

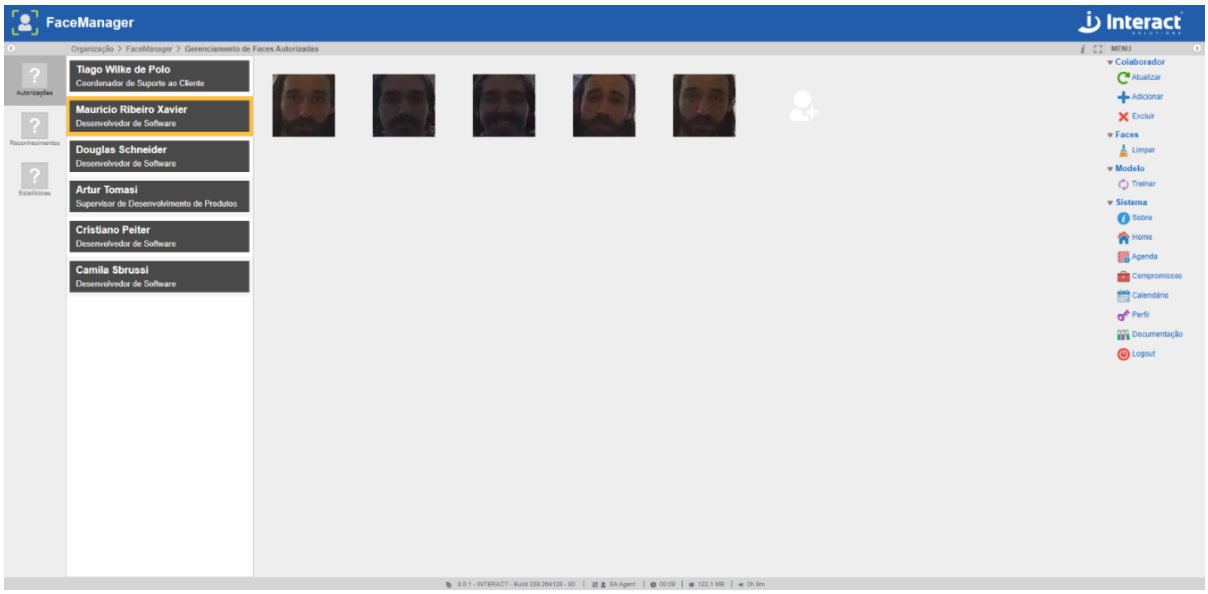
A seguir serão apresentadas as telas da aplicação de gerenciamento e o detalhamento das funcionalidades presentes em cada *view* disponibilizada na ferramenta.

4.3.1 Registro de faces autorizadas

Como pode ser observado na Figura 17, a *view* Autorizações possibilita aos gestores realizarem o gerenciamento das faces que estão autorizadas a acessar as dependências da empresa. Em um primeiro momento, devem ser adicionados os usuários do sistema *Strategic Adviser*, para que depois sejam vinculadas as imagens correspondentes de cada indivíduo.

Após finalizar o processo de configuração das faces autorizadas, os gestores poderão acionar o botão Treinar Modelo, que irá realizar o armazenamento das faces registradas em um diretório no servidor onde está a aplicação de reconhecimento facial. Após isto, o *script* responsável pela alimentação dos modelos será acionado via requisição REST para executar sua função.

Figura 17 – Interface da funcionalidade de registro de faces autorizadas

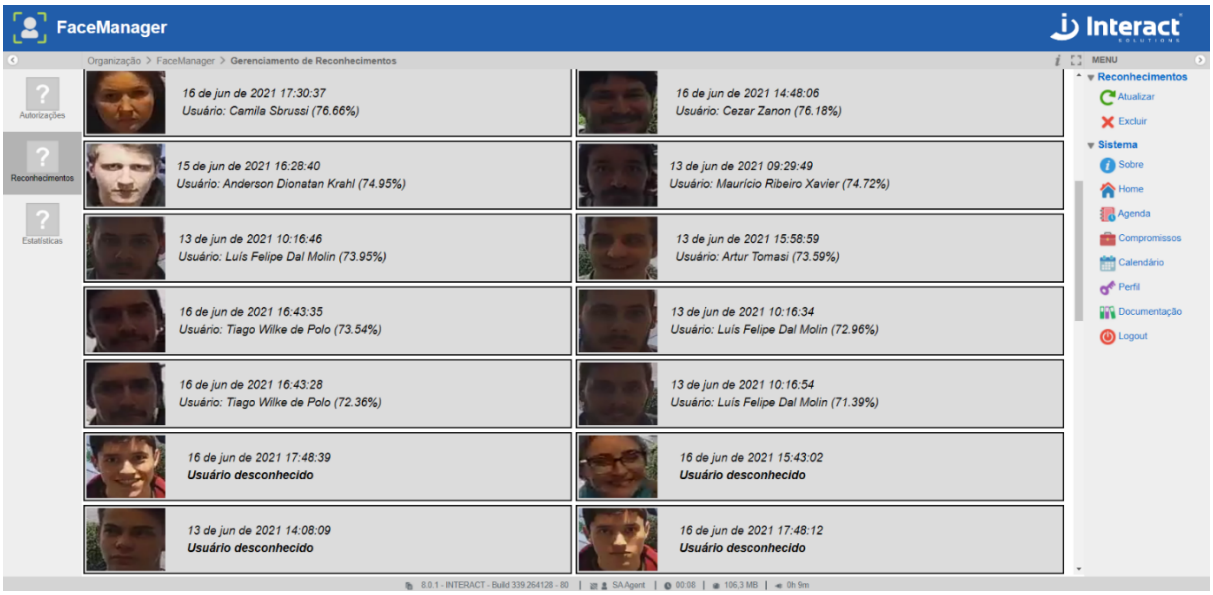


Fonte: Do autor (2021).

4.3.2 Registros de reconhecimentos

Conforme a Figura 18, a *view* Reconhecimentos tem como principal função a exibição das ocorrências de reconhecimento facial com as informações de assertividade, nome do usuário, data e hora do reconhecimento e o resultado da predição.

Figura 18 - Interface dos registros de reconhecimentos

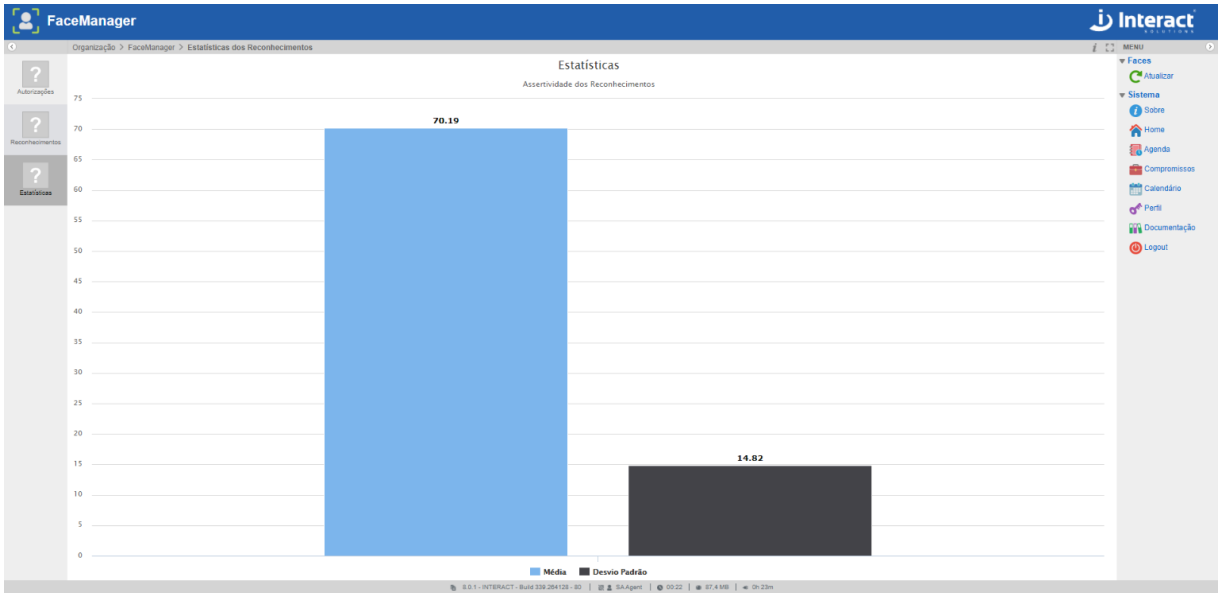


Fonte: Do autor (2021).

4.2.3 Estatísticas dos reconhecimentos

A view de Estatísticas (Figura 19) tem a finalidade de exibir aos gestores dados matemáticos como média e desvio padrão, acerca da assertividade registrada nas ocorrências de reconhecimento.

Figura 19 – Interface das estatísticas dos reconhecimentos



Fonte: Do autor (2021).

A implementação das funcionalidades incorporadas na aplicação e apresentadas neste capítulo teve como foco atender aos requisitos e necessidades observadas na etapa de planejamento do sistema. A ferramenta como um todo desempenhou de maneira adequada todas as etapas mencionadas, executando a detecção e reconhecimento facial dos usuários e possibilitando a administração dos registros de reconhecimento e do modelo de faces autorizadas.

No capítulo a seguir, serão detalhados o processo de testes da ferramenta desenvolvida, aplicado junto aos gestores e colaboradores da empresa, e a avaliação quantitativa das informações coletadas, possibilitando assim uma análise da efetividade da solução.

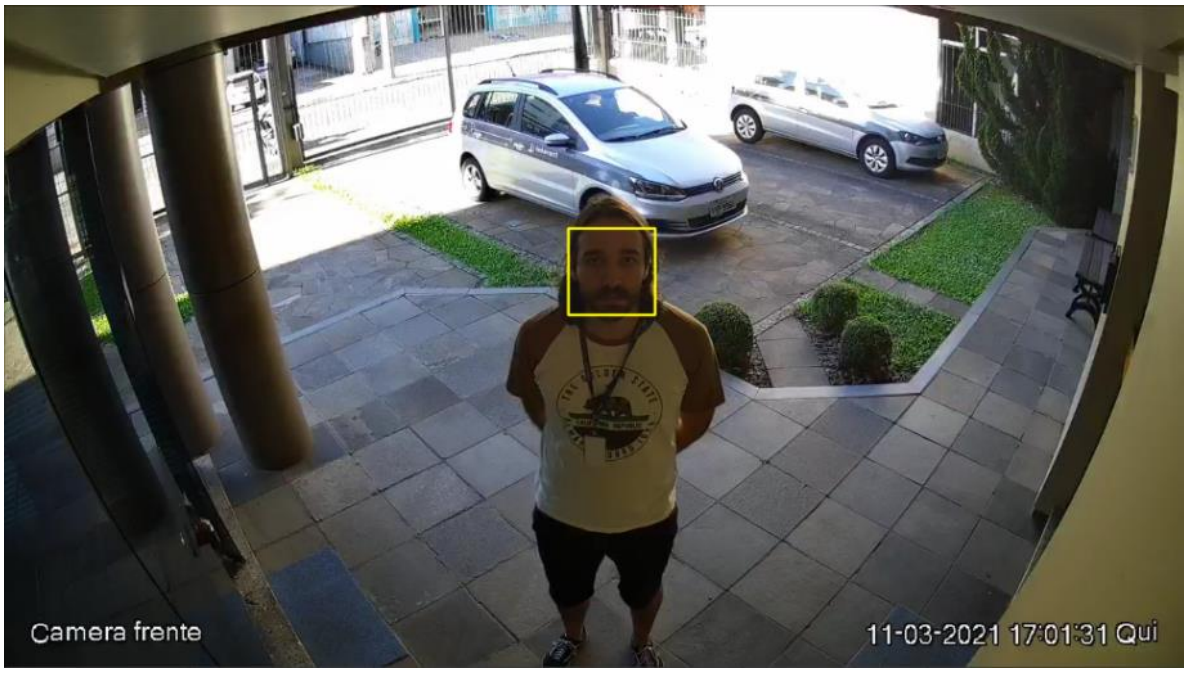
5 TESTES E ANÁLISE DOS RESULTADOS

Neste capítulo serão detalhados o processo de testes da ferramenta de reconhecimento facial e a análise dos resultados obtidos. Trata-se de uma etapa fundamental para validar a abordagem utilizada no desenvolvimento da aplicação em relação à resolução do problema proposto.

5.1 Abordagem dos testes

O processo de testagem da ferramenta iniciou-se com a seleção de 26 colaboradores das áreas de Clientes e Serviços, Produtos e Desenvolvimento, Administração e Negócios Internacionais, lotados nos setores de Desenvolvimento de Projetos, Suporte ao Cliente, Análise de Produtos, Desenvolvimento de Produtos, Design e Qualidade do Produto. Os colaboradores foram contatados individualmente em dias e horários distintos e acompanhados até a câmera, que está localizada ao lado da porta de entrada principal da empresa, conforme observado na Figura 20, para que as imagens de suas faces fossem capturadas e encaminhadas ao processo de reconhecimento. Após coletar todas as amostras, foi disponibilizado, por 2 dias, um questionário de avaliação da experiência da atividade de biometria facial, do ponto de vista do usuário final.

Figura 20 – Captura das faces através da câmera de vigilância



Fonte: Do autor (2021).

Em um segundo momento, para realizar a avaliação dos resultados da aplicação, 2 gestores da área de Produtos e Desenvolvimento foram convidados para testar a ferramenta de gerenciamento, durante um período de 2 dias. Foi requisitado a eles que fizessem a validação, observando principalmente os pontos mais críticos relacionados à assertividade dos registros e o nível de complexidade na condução das ações da aplicação. Em seguida, foi encaminhado a eles um questionário para que pudessem registrar suas observações acerca do uso da ferramenta.

Por último, foram selecionadas 3 amostras de contextos distintos, a fim de analisar o grau de assertividade da aplicação. Foi estabelecida como medida de avaliação da assertividade uma porcentagem, que levou em consideração o valor de *confidence* das ocorrências de reconhecimento e o valor limiar máximo definido pela ferramenta, conforme abordado anteriormente. Desta forma, quanto mais próximo de 0 for o valor de *confidence*, maior será a porcentagem de assertividade do reconhecimento, conforme Equação 5:

$$assertividade = 100 - \frac{confidence.100}{valor\ limiar} \quad (5)$$

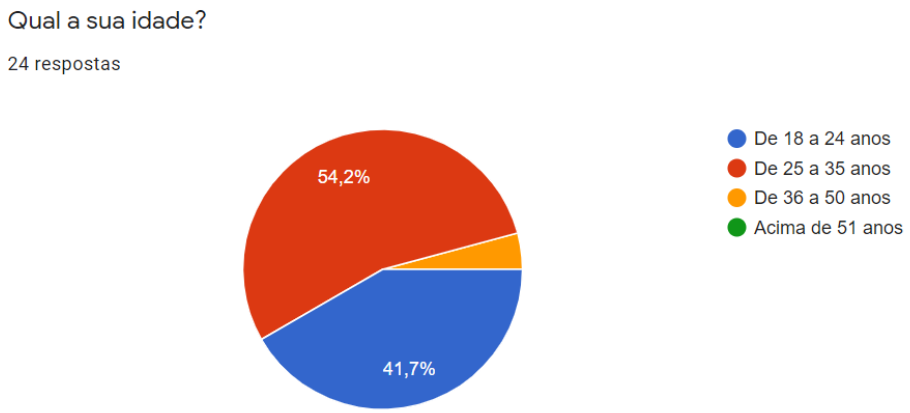
A seguir serão detalhadas a percepção dos colaboradores e gestores da empresa após as etapas dos testes realizados, assim como as amostras utilizadas para a aplicação da análise quantitativa dos dados.

5.2 Etapa 1 – Análise da experiência dos colaboradores

O questionário de avaliação da experiência com o processo de reconhecimento facial, do ponto de vista do usuário final, detalhado no Apêndice A foi elaborado e disponibilizado aos 26 colaboradores que participaram das validações da ferramenta, por um período de 2 dias. Houve a colaboração de 24 pessoas, que resulta em 92,31% dos convidados.

Conforme apresentado na Figura 20, a primeira questão possibilita identificar as faixas etárias das pessoas que participaram do processo de reconhecimento facial, a fim de incrementar o conteúdo e possibilitar diferentes análises das questões relacionadas diretamente com o processo de reconhecimento facial. Para esta pergunta, 41,7% responderam ter de 18 a 24 anos, 54,2% de 25 a 35 anos e 4,1% de 36 a 50 anos.

Figura 21 – Idade dos colaboradores



Fonte: Do autor (2021).

É possível observar na Figura 21 que a maior parte dos participantes são de uma geração que nasceu inserida no contexto da tecnologia, o que pode resultar em uma maior aceitação de técnicas como o reconhecimento facial. Por outro lado,

há um percentual de colaboradores pertencentes a uma geração “híbrida”, com relação a adaptação e utilização de novas tecnologias, desta forma, podendo apresentar maiores variações de opinião neste aspecto.

A questão presente na Figura 22 tem como propósito avaliar a aceitação dos usuários com relação ao uso do reconhecimento facial como forma de acesso ao seu local de trabalho. Esta análise possibilita uma relação com a questão anterior, na qual o percentual das respostas foi bastante similar, levando em consideração o contexto da idade. Para este questionamento, 91,7% responderam de forma afirmativa e 8,3% de forma negativa.

Figura 22 – Aceitação dos participantes com relação ao reconhecimento facial

Fonte: Do autor (2021).

Conforme demonstrado na Figura 22, a grande maioria dos colaboradores considerou a técnica de reconhecimento não invasiva. Este resultado pode estar diretamente relacionado ao fator da idade ou ao fato destas pessoas trabalharem no setor tecnológico.

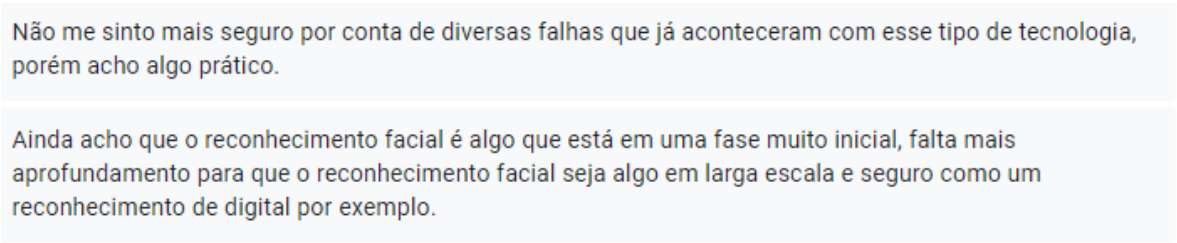
A Figura 23 apresenta um questionamento acerca da percepção dos usuários em relação a segurança. A finalidade desta questão é verificar se as pessoas acreditam que há um incremento na segurança, a partir da implantação de um sistema de controle de acesso baseado no reconhecimento facial. Para esta pergunta, 83,3% responderam de forma afirmativa e 16,7% de forma negativa.

Figura 23 – Aceitação dos participantes com relação a segurança

Fonte: Do autor (2021).

Pode-se observar que grande parte dos participantes considera como efetiva a aplicação de um sistema de controle de acesso, baseado em reconhecimento facial, para o aumento da segurança. As justificativas para as respostas negativas levam em consideração o fato de que, alguns projetos de reconhecimento facial já apresentaram graves falhas e as pesquisas relacionadas a este tipo de tecnologia ainda são insuficientes, conforme Figura 24.

Figura 24 – Justificativas para a falta de segurança com o reconhecimento facial



Fonte: Do autor (2021).

A próxima questão tem relação direta com o contexto de pandemia, que se deu durante o desenvolvimento deste estudo. Buscou-se analisar a remoção da máscara como fator que gera incomodo para os colaboradores, no momento do reconhecimento. Conforme observado na Figura 25, 95,8% dos participantes responderam negativamente, enquanto 4,2% sentiram algum tipo de incômodo.

Figura 25 – Avaliação dos participantes com relação a remoção da máscara

Fonte: Do autor (2021).

A grande maioria dos participantes relatou que não houve motivos para preocupação com a remoção da máscara, visto que os protocolos de distanciamento foram respeitados. Além disso, houve relatos de que o ambiente onde o processo de reconhecimento foi aplicado estava em uma área aberta, com bastante circulação de ar. Por outro lado, alguns dos colaboradores reportaram que caso houvesse uma movimentação muito intensa de pessoas, seria incomodo retirar o acessório.

O questionamento seguinte foi formulado com o intuito de analisar a percepção dos usuários em relação ao tempo gasto para o reconhecimento facial. Conforme figura 26, 91,7% dos colaboradores responderam positivamente e 8,3% de forma negativa.

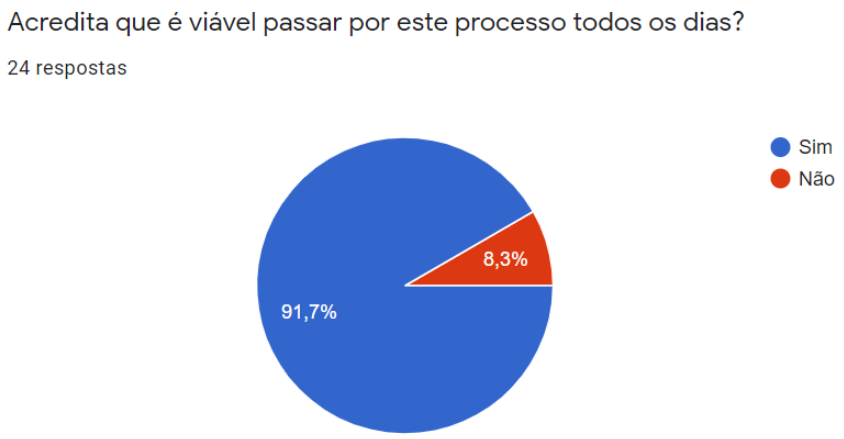
Figura 26 – Avaliação dos participantes com relação ao tempo para o reconhecimento

Fonte: Do autor (2021).

Os colaboradores avaliaram de maneira preponderante que o tempo para o reconhecimento foi adequado, inclusive realizando comparações com outras formas de controle de acesso, como a inserção manual de senhas e a biometria pela impressão digital. No entanto, os participantes que responderam esta questão negativamente, relataram que em momentos de muita movimentação de pessoas, a necessidade de remover os acessórios e virar-se para a câmera, pode resultar em um tempo total demasiado.

A Figura 27 apresenta uma pergunta que foi elaborada com a intenção de extrair dos colaboradores sua percepção em relação a viabilidade de aplicar o processo de reconhecimento facial todos os dias, para controlar o acesso à empresa. As repostas foram 91,7% positivas e 8,3% negativas.

Figura 27 – Avaliação dos participantes com relação a viabilidade de aplicação da ferramenta diariamente



Fonte: Do autor (2021).

Os participantes que responderam positivamente justificaram que, pelo fato de realizar o reconhecimento de forma segura, ágil e a atividade não impactar na rotina dos indivíduos, é perfeitamente viável a aplicação diária da ferramenta. Contudo, alguns colaboradores relataram que é necessária uma maior agilidade no processo de reconhecimento para que se torne uma ferramenta viável.

Por fim, foi solicitado aos colaboradores que contribuíssem com sugestões e observações a respeito da experiência com a ferramenta de reconhecimento facial para que possíveis melhorias possam ser implementadas futuramente

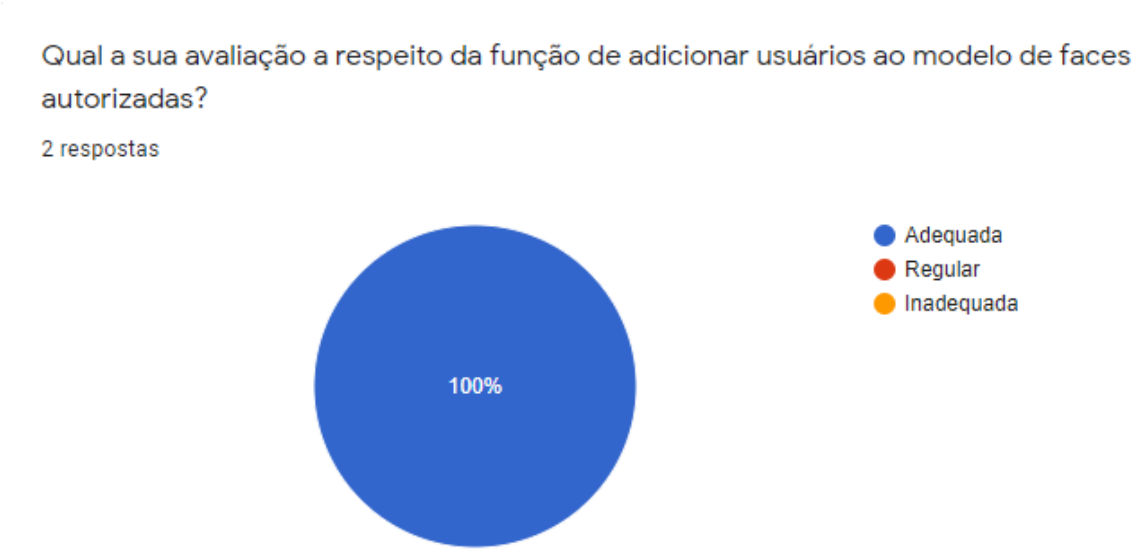
Os participantes propuseram melhorias no sistema para que o reconhecimento seja efetuado sem que a pessoa necessite parar em frente a câmera, agilizando o processo. Além disso, foi sugerida a inclusão de alguma forma de *feedback* que informe o posicionamento correto do usuário e indique se o reconhecimento foi efetivo ou não. Também houve comentários em relação ao uso de acessórios e a sugestão de um aperfeiçoamento na detecção de faces com a utilização destes.

5.3 Etapa 2 – Análise da aplicação por parte dos gestores

O questionário de avaliação da aplicação de gerenciamento para o processo de reconhecimento facial, detalhado no Apêndice B, foi disponibilizado aos 2 gestores do setor de Desenvolvimento de Produtos. Para responder ao questionário, os gestores foram instruídos a utilizar a aplicação e explorar todas as suas funcionalidades.

Conforme apresentado na Figura 28, a primeira questão proporciona uma análise acerca da percepção dos gestores em relação a função de alimentação do modelo de faces autorizadas. Para esta pergunta, 100% das respostas indicam que a funcionalidade é adequada.

Figura 28 - Avaliação dos gestores com relação a funcionalidade de adicionar usuários ao modelo de faces autorizadas



Fonte: Do autor (2021).

As justificativas para as respostas apresentadas na Figura 28 indicam que a funcionalidade atende ao que se propõe de maneira bastante intuitiva. Como sugestão de melhoria para versões futuras, foi proposta a possibilidade de inserção de faces autorizadas de pessoas que não fazem parte do quadro de colaboradores

da empresa. Segundo os participantes, esta melhoria possibilitaria o cadastro de clientes ou convidados que frequentemente visitam a empresa.

A questão exibida na Figura 29 tem como objetivo possibilitar uma análise a respeito de qual a avaliação dos gestores com relação a assertividade atingida pela ferramenta. Nesta questão, 100% das respostas apontam que a assertividade geral da ferramenta está adequada.

Figura 29 – Avaliação dos gestores com relação ao nível de assertividade da ferramenta

Fonte: Do autor (2021).

Os participantes justificaram que a assertividade geral da ferramenta foi satisfatória, considerando o conjunto de reconhecimentos presentes na aplicação nos momentos em que foi utilizada. É importante destacar que não havia ocorrências de reconhecimento de colaboradores com máscara no momento da avaliação dos gestores, circunstância que diminui a assertividade principalmente para pessoas que não possuem imagens com máscara registradas no modelo de faces autorizadas.

Na Figura 30 é possível observar o questionamento que tem como objetivo verificar se na opinião dos gestores a ferramenta de reconhecimento facial contribui para aprimorar a segurança na empresa. As repostas para esta pergunta foram 100% afirmativas.

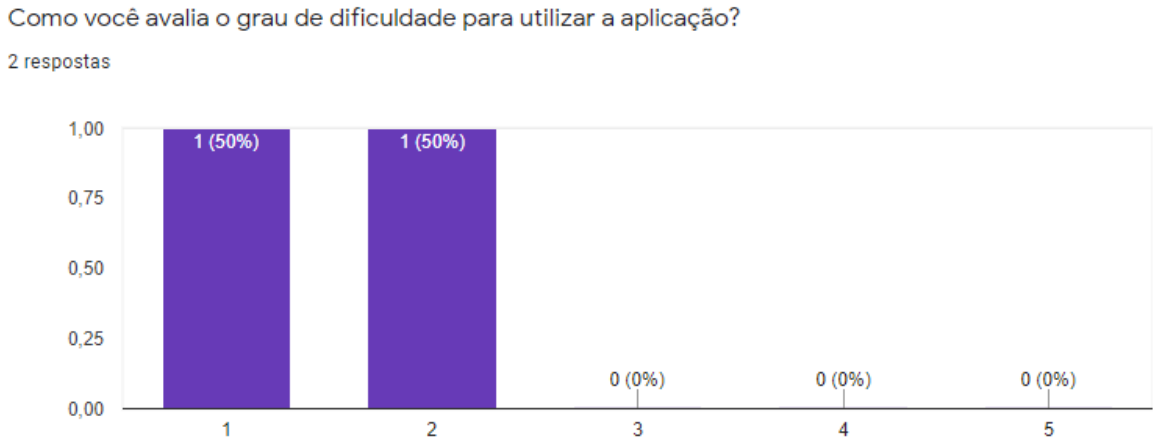
Figura 30 – Avaliação dos gestores com relação a melhora do nível de segurança da empresa

Fonte: Do autor (2021).

Para os gestores, a ferramenta auxilia nos processos relacionados ao controle de acesso da empresa possibilitando monitorar e administrar a entrada de pessoas a partir das informações presentes na aplicação. Neste aspecto, foram sugeridas a apresentação de estatísticas que possibilitem observar a quantidade de reconhecimentos não autorizados, além da disponibilização de filtros para exibir informações mais específicas em tela.

O questionamento presente na Figura 31 tem a finalidade de observar, a partir das respostas dos participantes, se o nível de complexidade da aplicação está adequado para atingir os objetivos propostos. É importante ressaltar que quanto menor o nível selecionado pelo participante, menor a dificuldade avaliada. Desta forma, 50% das respostas indicam uma dificuldade de grau 1 e 50% apontam para uma dificuldade de grau 2.

Figura 31 - Avaliação dos gestores com relação ao grau de dificuldade para utilizar a aplicação



Fonte: Do autor (2021).

Os gestores justificaram as respostas apresentadas na Figura 31 relatando que a aplicação é bastante simples e intuitiva, e que a disposição das funcionalidades disponibilizadas facilita a usabilidade da ferramenta. Para auxiliar ainda mais com as questões relacionadas a usabilidade, foi sugerida a incorporação de dicas às telas da aplicação.

Ao final do questionário os participantes contribuíram com sugestões e observações que podem auxiliar na evolução da aplicação para as próximas versões. Neste sentido, foi sugerida a implementação de mais indicadores que possibilitem a visualização com mais detalhes dos resultados das ocorrências de reconhecimento. Além disso, foi proposta a implementação de uma funcionalidade que permita ao gestor definir se um reconhecimento foi correto ou não e partir destes dados incrementar o modelo de faces autorizadas.

5.4 Análise das amostras

Para realizar a análise quantitativa das ocorrências de reconhecimento facial registradas na aplicação, foram realizadas análises tendo como base 3 conjuntos de registros diferentes. Os indicadores utilizados para auxiliar na análise das

informações foram extraídos das métricas de avaliação abordadas anteriormente no trabalho. Em conjunto com os gestores foi definido que as ocorrências com assertividade acima de 70% caracterizam um reconhecimento verdadeiro positivo, os valores abaixo representam os reconhecimentos falso negativos.

Com o objetivo de incrementar a análise quantitativa, foram utilizados os indicadores de média e desvio padrão para possibilitar uma avaliação do comportamento das ocorrências de reconhecimento facial como um todo.

Larson e Farber (2015) afirmam que a média se refere a uma medida que possibilita uma análise central de um conjunto de dados, sendo calculada a partir da soma de cada elemento dividida pelo número total de registros dentro de uma amostra ou população. Em relação ao desvio padrão, os autores acrescentam que o desvio em um conjunto de dados é representado pela distância entre este e a média, portando o desvio padrão expressa a variabilidade dos dados em relação à média.

5.4.1 Amostra 1 – Assertividade geral da aplicação

Esta amostra apresenta os dados relacionados às ocorrências de reconhecimento facial de 24 colaboradores. Foram coletados 53 registros durante um período de 3 dias de testes. Para que a amostragem se aproximasse ao máximo da realidade, os registros foram coletados em horários diferentes e em dias em que a intensidade da luz foi bastante variada. As informações coletadas podem ser observadas no Quadro 3.

Como pode ser verificado no Quadro 3, a assertividade média geral das ocorrências de reconhecimento facial superou o valor mínimo aceitável, mencionado anteriormente, de 70%.

Quadro 3 – Dados da Amostra 1

	Resultados
Verdadeiros Positivos	31
Falsos Negativos	22
Taxa de Aceitação Falsa (FAR)	41.50%
Média (Assertividade)	70.49%
Desvio Padrão (Assertividade)	14.14%

Fonte: Do autor, (2021).

No entanto, é possível analisar, a partir da medida de desvio padrão, que os registros do modelo estão bastante dispersos, o que caracteriza uma grande quantidade de ocorrências com assertividade alta e outra grande parte dos registros com assertividade baixa, valores que são confirmados pelos indicadores de verdadeiros positivos e falsos negativos. Neste sentido, se faz necessária a elaboração de novas estratégias com foco na diminuição de registros falsos negativos.

5.4.2 Amostra 2 – Assertividade da aplicação para colaboradores utilizando máscaras

A análise desta amostra conta com os registros de 5 colaboradores utilizando máscaras no momento da detecção facial. Os registros foram separados em dois grupos para uma melhor interpretação dos dados. No primeiro grupo estão 2 colaboradores que possuem imagens com máscara registradas no modelo de faces autorizadas. No segundo grupo estão presentes os 3 usuários restantes somente com imagens sem máscara registradas.

No Quadro 4 é possível observar as informações de 10 registros de reconhecimento facial do grupo de colaboradores que possuem imagens com máscara registradas no modelo de faces autorizadas.

Quadro 4 – Dados da Amostra 2 para o primeiro grupo

	Resultados
Verdadeiros Positivos	5
Falsos Negativos	5
Taxa de Aceitação Falsa (FAR)	50%
Média (Assertividade)	60.48%
Desvio Padrão (Assertividade)	27.21%

Fonte: Do autor, (2021).

Analisando os dados do grupo de colaboradores, detalhados no Quadro 4, é possível observar que a ferramenta apresenta um nível de assertividade plausível, considerando que esta amostra contém somente registros de colaboradores utilizando máscaras e que não houve nenhuma implementação na ferramenta com relação a este acessório. Contudo, é importante destacar que, caso o reconhecimento de colaboradores com máscara seja efetivado, melhorias são necessárias para aumentar a assertividade média das ocorrências e diminuir a dispersão dos registros no conjunto de dados.

O Quadro 5 apresenta os dados de 13 ocorrências de reconhecimento facial do grupo de colaboradores que não possuem imagens com máscara registradas no modelo de faces autorizadas.

Quadro 5 - Dados da Amostra 2 para o segundo grupo (Continua)

	Resultados
Verdadeiros Positivos	0

Quadro 5 - Dados da Amostra 2 para o segundo grupo (Conclusão)

Falsos Negativos	13
Média (Assertividade)	10.97%
Desvio Padrão (Assertividade)	10.40%

Fonte: Do autor, (2021).

Observa-se no Quadro 5, que em nenhuma ocorrência foi possível obter uma assertividade aceitável. Neste contexto, em comparação com o outro grupo de colaboradores analisado, é possível afirmar que o cadastro das imagens no padrão correto tem relação direta com o aumento da assertividade das predições.

Considerando a avaliação de experiência e da ferramenta por parte dos colaboradores e gestores em conjunto com a análise quantitativa das amostras selecionadas, é possível concluir que a solução atingiu resultados satisfatórios perante o problema de pesquisa proposto, possibilitando a utilização definitiva da ferramenta no controle de acesso às dependências da empresa.

6 CONCLUSÃO

A segurança dos colaboradores e patrimônio privado sempre foi um tema de grande relevância entre as instituições. Apesar da grande evolução tecnológica observada nas últimas décadas nesta área, algumas organizações apresentam certa dificuldade ou receio para modernizar suas ferramentas. Neste sentido, o avanço dos estudos relacionados às técnicas de reconhecimento facial surge como uma alternativa viável para possibilitar a atualização destes estabelecimentos no que se refere à segurança no contexto do controle de acesso.

A proposta apresentada objetivou o desenvolvimento e avaliação de uma ferramenta de reconhecimento facial, vinculada a um sistema de gestão, que permite a administração e monitoramento do acesso de pessoas em uma empresa de tecnologia. A aplicação utiliza os algoritmos presentes na biblioteca de visão computacional OPENCV, para possibilitar a alimentação do modelo de pessoas autorizadas e aplicar predições de acordo com que novas faces são capturadas.

Levando em consideração a avaliação da experiência de reconhecimento facial por parte dos colaboradores da empresa, é possível destacar que a grande maioria dos participantes considera positiva a implantação de um sistema deste porte na organização, destacando pontos como uma maior segurança e agilidade durante as etapas de funcionamento da ferramenta.

A avaliação da ferramenta por parte dos gestores evidencia que a solução desenvolvida é bastante intuitiva, possibilitando a utilização das funções disponibilizadas de uma maneira simples e efetiva. Além disso, os gestores

concluem que as informações apresentadas na aplicação auxiliam no monitoramento e administração do acesso à empresa, possibilitando a elaboração de planos de ação em caso de alguma inconformidade.

A partir da análise dos dados quantitativos gerados pela aplicação é possível concluir que a ferramenta é eficaz na solução do problema que se propôs a resolver, visto que a assertividade média das ocorrências de reconhecimento superou o mínimo de 70% definido juntamente com os gestores. No entanto, é importante ressaltar que a alta dispersão dos dados dentro das amostras analisadas apresenta-se como um problema a ser resolvido em versões futuras da ferramenta para aumentar sua confiabilidade.

Levando em consideração o contexto de pandemia que se apresenta nos dias de hoje, surge como uma sugestão para trabalhos futuros agregar a esta ferramenta o reconhecimento facial com a utilização de máscaras, eliminando assim a necessidade de remoção deste acessório no momento da detecção facial.

Com base neste estudo, é possível destacar que a área de visão computacional, sobretudo no contexto da biometria facial, dispõe de uma grande variedade de oportunidades de desenvolvimento de pesquisas que contribuam para a sociedade. Neste sentido, ferramentas para auxiliar instituições governamentais e particulares no processo de identificação de suspeitos ou controle da utilização de máscaras, em tempos de pandemia, apresentam-se como soluções viáveis de implementação empregando as mesmas tecnologias detalhadas neste trabalho.

REFERÊNCIAS

AYDIN, I.; OTHMAN, N. A. A New IoT Combined Face Detection of People by Using Computer Vision for Security Application. **International Artificial Intelligence and Data Processing Symposium (IDAP)**, p. 1-6, set. 2017.

BAKSHI, N.; PRABHU, V. Face Recognition System for Access Control using Principal Component Analysis**. International Conference on Intelligent Communication and Computational Techniques (ICCT),** Jaipur, p. 145-150, dez. 2017.

CARNEIRO, Larissa Natália das Virgens. **Reconhecimento de Face Invariante a Iluminação baseado em uma Abordagem Supervisionada**. Universidade Federal de Ouro Preto, 2012.

DINIZ, F. A.; MENDES NETO, F. M., LIMA JÚNIOR, F. C.; FONTES, L. M. O. RedFace: Um Sistema de Reconhecimento Facial para Identificação de Estudantes em um Ambiente Virtual de Aprendizagem. **Novas Tecnologias na Educação**, v. 10, p. 1-11, dez. 2012. Disponível em: <https://seer.ufrgs.br/renote/article/view/36403/23510>. Acesso em: 20 out., 2020.

FUJIKAWA, Cesar Shuji. **Reconhecimento Facial utilizando Descritores de Textura e Aprendizado Não Supervisionado.** Monografia (Graduação) - Curso de Ciências da Computação, Instituto de Geociências e Ciências Exatas, Rio Claro, 2016.

GERHARDT, Tatiane Engel; SILVEIRA, Denise Tolfo. **Metodologia da Pesquisa**. 1. ed. Porto Alegre: Editora da UFRGS, 2009. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 04 jan. 2018.

INTERACT SOLUTIONS LTDA. **SA Strategic Adviser**. Disponível em: <https://www.interact.com.br/>. Acesso em: 19 jun. 2021.

ISMAIL, N.; SABRI, M. I. Md. Mobile to Server Face Recognition: A System Overview. **World Academy of Science, Engineering and Technology**, v. 69, p.767-761, 2010.

JACOBSON, Sheldon H.; KOBZA, John E., NAKAYAMA, Marvin K. A sampling procedure to estimate risk probabilities in access-control security systems. **European Journal of Operational Research,** v. 122, n. 1, p. 123-132, abr. 2000.

JAIN, A.; BOOLE, Ruud; PANKANTI, Sharath. **Biometrics: Personal identification in networked society.** Springer: New York City, 2005.

JAIN, A. K.; FLYNN, P.; ROSS, A. A. **Handbook of biometrics.** Springer: New York City, 2007.

JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. **IEEE Transaction on Circuits and System for Video Technology**. V. 14, n. 1, p. 4-20, jan. 2004.

JIANG, J.; ZHANG, L; FURUKAWA, T. A class density approximation neural network for improving the generalization of Fisherface. **Neurocomputing**, v. 71, p. 3239–3246, jul. 2008.

KREMIC, E.; SUBASI, A.; HAKDAREVIC, K. Face Recognition Implementation for Client Server Mobile Application using PCA. **Int. Conf. Of Information Technology Interfaces**, Croácia, p.435-440, jun. 2012.

LABATI, R. D.; GENOVESE, A; MUÑOZ, E.; PIURI, V.; SCOTTI, F.; SFORZA, G. Computational Intelligence for Biometric Applications: A Survey. **International Journal of Computing**, v. 15, n. 1, p. 42-53, 2016.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica.** 7.ed. São Paulo: Atlas, 2010.

LIU, S.; SILVERMAN, M. A Practical Guide to Biometric Security Technology. **IT Professional**, v. 3, n. 1, p. 27–32, 2001.

LOZOYA-SANTOS, J de J.; SEPÚLVEDA-ARRÓNIZ, V.; TUDON-MARTINEZ, J. C., RAMIREZ-MENDOZA, R. A. Survey on biometry for cognitive automotive systems**. Cognitive System Research**, v. 55, p. 175-191, jan. 2019.

MASONA, J.; DAVEB, R.; CHATTERJEEC, P.; GRAHAM-ALLENA, I.; ESTERLINEA, A.; ROY, K. An Investigation of Biometric Authentication in the Healthcare. **Array**, v. 8, dez. 2020.

STYLIOS, I.; KOKOLAKIS, S.; THANOU, O.; CHATZIS, S. Behavioral biometrics & continuous user authentication on mobile devices: A survey. **Information Fusion,** v. 66, p. 76-99, fev. 2021.

MORAES, A. F.; CAMARGO JÚNIOR, J. B. **Método para avaliação da tecnologia biométrica na segurança de aeroportos.** 2006. Universidade de São Paulo, São Paulo, 2006.

NIU, G.; CHEN, Q. Learning an video frame-based face detection system for security fields.y. **Journal of Visual Communication and Image Representation**, v. 55, p. 457-463, aug. 2018.

OLIVEIRA GALIMBERTI, L. H. **ESTUDO COMPARATIVO DE ALGORITMOS DE BIOMETRIA FACIAL DISPONIBILIZADOS PELA BIBLIOTECA OPENCV PARA CONTROLE DE ACESSO.** 2018. Universidade do Vale do Taquari, Lajeado, 2018.

OPENCV. Open Source Computer Vision Library, Disponível em: <http://opencvlibrary.sourceforge.net/>. Acesso em: mar. 2021.

PRODANOV, C. A.; FREITAS, E. C. **Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho acadêmico.** 2. ed. Novo Hamburgo Rio Grande do Sul: Universidade FEEVALE, 2013.

RAMESWARI, R.; KUMAR, S. N.; AANANTH, M. A., DEEPAK, C. Automated access control system using face recognition. **Materials Today:** Proceedings. Sathyamangalam, p. 1-6, mar. 2020.

RON, Larson; FARBER, Betsy. Estatística aplicada. 1. Ed. São Paulo: Pearson Education do Brasil, 2015.

SAMPIERI, Hernández; COLLADO, Fernández; LUCIO, Baptista. **Metodologia de PESQUISA**. 5. ed. São Paulo: Penso Editora LTDA., 2013.

SANTOS, A. L. **Gerenciamento de identidades: segurança da informação.** 1. ed., Rio de Janeiro: Brasport, 2007.

SCHROFF, F.; KALENICHENKO, D.; PHILBIN, J. FaceNet: A Unified Embedding for Face Recognition and Clustering. **IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**, jun. 2015.

SOUZA, M. B. **Controle de acesso: conceitos, tecnologias e benefícios.** 1. Ed., São Paulo: Sicurezza Editora, 2010.

TASKIRAN, M.; KAHRAMAN, N.; ERDEM, C. E. Face recognition: Past, present and future. **Digital Signal Processing**, v. 106, nov. 2020.

VIOLA, P.; JONES, M. Rapid Object Detection using a Boosted Cascade of Simple Features. **Conference on Computer Vision and Patterns Recognition**, v. 1, p. 1-9, 2001.

ZHAO, W.; CHELLAPA, R.; PHILLIPS, P. J.; ROSENFELD, A. Face Recognition: A Literature Survey. **ACM Computing Surveys**, v. 35, n. 4, p. 399–458, dez. 2003.

PYTHON. Programmig language, 2020. Tópico temático. Site corporativo. Disponível em: <https://www.python.org/>. Acesso em: 04 nov. 2020.

APÊNDICES

APÊNDICE A – Questionário de avaliação da experiência de reconhecimento facial para controle de acesso

1 - Qual a sua idade?
( ) De 18 a 24 anos
( ) De 25 a 35 anos
( ) De 36 a 50 anos
( ) Acima de 51 anos

2 - Você considera a técnica de reconhecimento facial invasiva?
( ) Sim
( ) Não

3 - Você se sente mais seguro com a adoção do reconhecimento facial para o controle de acesso?
( ) Sim
( ) Não

4 - Você se sentiu incomodado ao retirar a máscara durante o processo de reconhecimento facial?
( ) Sim
( ) Não

5 – Você acha que o tempo gasto para o processo de reconhecimento facial foi adequado?
( ) Sim
( ) Não

6 - Acredita que é viável passar por este processo todos os dias?
( ) Sim
( ) Não

7 - Sugestões e/ou observações?

APÊNDICE B – Questionário de avaliação da aplicação de gerenciamento do reconhecimento facial (gestores)

1 - Qual a sua avaliação a respeito da função de adicionar usuários ao modelo de faces autorizadas?

( ) Adequada

( ) Regular

( ) Inadequada

2 - Qual a sua avaliação a respeito do nível de assertividade da ferramenta?

( ) Adequada

( ) Regular

( ) Inadequada

3 - Você acredita que esta ferramenta proporciona mais segurança à empresa?

( ) Sim

( ) Não

4 - Como você avalia o grau de dificuldade para utilizar a aplicação?

( ) 1

( ) 2

( ) 3

( ) 4

( ) 5

5 - Sugestões e/ou observações?