

ROBSON ALMEIDA BORGES DE FREITAS

**AMBIENTES VIRTUAIS DE APRENDIZAGEM COM BIOMETRIA
FACIAL**

**Recife
2016**



Universidade Federal Rural de Pernambuco
Unidade Acadêmica de Educação a Distância e Tecnologia
Pró-Reitoria de Pesquisa e Pós-Graduação
Programa de Pós-Graduação em Tecnologia e Gestão em Educação a Distância

AMBIENTES VIRTUAIS DE APRENDIZAGEM COM BIOMETRIA FACIAL

Dissertação apresentada ao Programa de Pós-Graduação em Tecnologia e Gestão em Educação a Distância como exigência parcial à obtenção do título de Mestre em Tecnologia e Gestão em Educação a Distância.

Linha de Pesquisa: Ferramentas Tecnológicas para Educação a Distância.

Orientador: Prof. Dr.: Rodrigo Nonamor Pereira Mariano de Souza

Recife

2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

F866a Freitas, Robson Almeida Borges de
Ambientes virtuais de aprendizagem com biometria facial /
Robson Almeida Borges de Freitas. – 2016.
118 f. : il.

Orientador: Rodrigo Nonamor Pereira Mariano de Souza.
Dissertação (Mestrado) – Universidade Federal Rural de
Pernambuco, Programa de Pós-Graduação em Tecnologia e Gestão
em Educação a Distância, Recife, BR-PE, 2016.
Inclui referências e apêndice(s).

1. Educação a distância 2. Ambiente virtual de aprendizagem
3. Reconhecimento facial. 4. Biometria facial 5. Segurança da
informação I. Souza, Rodrigo Nonamor Pereira Mariano de, orient.
II. Título

CDD 371.394422

Universidade Federal Rural de Pernambuco
Unidade Acadêmica de Educação a Distância e Tecnologia
Pró-Reitoria de Pesquisa e Pós-Graduação
Programa de Pós-Graduação em Tecnologia e Gestão em Educação a Distância

AMBIENTES VIRTUAIS DE APRENDIZAGEM COM BIOMETRIA FACIAL

ROBSON ALMEIDA BORGES DE FREITAS

Dissertação julgada adequada para obtenção do título de Mestre em Tecnologia e Gestão em Educação a Distância, defendida e aprovada por unanimidade em 28/11/2016 pela Banca Examinadora.

Orientador:

Prof. Dr. Rodrigo Nonamor Pereira Mariano de Souza
Programa de Pós-Graduação em Tecnologia e Gestão em Educação a Distância -
UFRPE

Banca Examinadora:

Prof^a. Dr^a. Marizete Silva Santos
Membro Interno – Programa de Pós-Graduação em Tecnologia e Gestão em
Educação a Distância - UFRPE

Prof^a. Dr^a. Juliana Regueira Basto Diniz
Membro Interno – Programa de Pós-Graduação em Tecnologia e Gestão em
Educação a Distância - UFRPE

Prof. Dr. Filipe Rolim Cordeiro
Membro Externo – Programa de Pós-Graduação em Informática Aplicada –
Departamento de Estatística e Informática - UFRPE

Dedico este trabalho a todos que contribuíram com minha formação, seja de forma positiva ou negativa, pois com isso aprendi na prática o verdadeiro significado e a diferença de cada uma dessas palavras: insistir, desistir e persistir.

AGRADECIMENTOS

Agradeço primeiramente ao Deus criador e distribuidor do equilíbrio universal que de forma sábia permeia nossas vidas de escolhas e através delas adquirimos sabedoria ou caímos no vazio da ignorância. Agradeço a Deus por ter me dado o senso do exemplo e saber que por mais que algumas pessoas insistam em nos desapontar, o único legado que podemos deixar é o exemplo a ser seguido.

Agradeço de forma impessoal ao tempo que rege os nossos caminhos, e através do qual podemos dedicar parte do tempo que nos pertence a nossa família, nossos irmãos, filhos, mãe, pai e esposa, dividindo sorrisos, alegrias e tristezas com nossos amigos. Além disso, podemos dedicar nosso tempo ao aprendizado e ao ensino, que é a parte divina que está ao nosso alcance, e saber que com o conhecimento podemos perdoar, conquistar, amar, viver e criar a vida no nosso mundo.

Agradeço pelo que recebo do seio familiar, representado pela atenção e presença da minha mãe; pelo foco, disciplina e compromisso dado pelo meu pai; o senso de responsabilidade e fraternidade dado pelas minhas irmãs; a minha filha e a minha esposa que me trouxeram de volta a vida e a luz em um momento de escuridão.

Obrigado a todos os amigos, professores, orientadores, colegas de trabalho e colegas do mestrado. Nada na vida é fácil ou dado, e essa conquista é realização de todos. Muito Obrigado!

“O papel do professor é criar as condições para a invenção, em lugar de fornecer conhecimentos já consolidados.”

(Seymour Papert)

RESUMO

A Educação a Distância tem obtido grande importância no cenário educacional brasileiro. Através da facilidade de acesso às novas Tecnologias de Informação e Comunicação, tem-se expandido em alcance geográfico e numérico. Com isso, a Educação a Distância vem democratizando o ensino e o conhecimento, levando-os para áreas remotas em que o ensino presencial encontra inúmeras dificuldades para atender a população. O desenvolvimento de ferramentas que auxiliem na qualidade dos Ambientes Virtuais de Aprendizagem (AVA) tem se tornado uma prática para melhorar a Educação a Distância. O tópico da presente pesquisa é Segurança da Informação nos AVAs, tendo como hipótese que a biometria facial pode contribuir com esse aspecto através do monitoramento dos alunos nas plataformas virtuais de ensino em cursos na modalidade de Educação a Distância. Nossa proposta é melhorar o procedimento de autenticação na plataforma com a utilização da biometria facial, possibilitando a verificação da presença desse aluno com o reconhecimento facial. O estudo foi composto de três etapas. Na primeira etapa foi realizada uma pesquisa bibliográfica. Na segunda etapa foi realizado a elaboração e aplicação de um questionário para os integrantes da EAD do Instituto Federal do Piauí e da Universidade Federal do Piauí, no qual detectamos uma opinião positiva sobre a criação de novas ferramentas de autenticação. Partindo-se da pesquisa bibliográfica e da análise dos dados coletados através do questionário, a terceira etapa consistiu no desenvolvimento de um protótipo de reconhecimento facial para os AVAs. Participaram da pesquisa um total de 83 indivíduos, entre estudantes, tutores presenciais, tutores a distância, coordenadores, professores conteudistas e professores pesquisadores. Como inovação tecnológica para a Educação a Distância, nosso protótipo de reconhecimento facial foi implementado com as linguagens PHP e PYTHON, e a biblioteca de visão computacional OPENCV para detecção facial com *haarcascade* e reconhecimento facial com Padrões Binários Locais de Histogramas (LBPH). A ferramenta foi desenvolvida de forma a reconhecer o aluno através de padrões faciais, registrando a sua presença nos Ambientes Virtuais de Aprendizagem. Nos testes do protótipo foi utilizado um banco de dados com 167 imagens, além da realização do cadastro e reconhecimento de 20 usuários e testes de simulação de fraudes. Para testes de desempenho foi montado um banco de dados com 226 imagens. O protótipo demonstrou eficiência no desempenho e na efetivação do reconhecimento facial dos usuários, embora necessite de novas implementações.

Palavras-chave: Educação a Distância; Ambiente Virtual de Aprendizagem; Reconhecimento Facial; Biometria Facial; Segurança da Informação.

ABSTRACT

Online education has achieved great importance in Brazil's education. Through the ease of access to the new Information and Communication Technologies, it has expanded in geographical and numerical reach. This way, Online Education has been democratizing teaching and knowledge, taking them to remote areas where face-to-face teaching encounters numerous difficulties in serving the population. The development of tools that support the quality of Virtual Learning Environments (VLE) has become frequent in order to improve Online Education. The topic of this research is Information Security in VLEs, and its hypothesis is that facial biometry can contribute to this aspect through the monitoring of students in the virtual platforms of teaching in courses in the modality of Online Education. Our proposal is to improve the authentication procedure on the pallet with the use of facial biometrics, enabling a verification of the vision with facial recognition. The study was composed of three stages. In the first stage, a bibliographical research was carried out. In the second stage, a questionnaire was developed and applied to the Online Education members at Instituto Federal do Piauí and Universidade Federal do Piauí, in which we detected a positive opinion about the creation of new authentication tools. Based on the bibliographical research and the analysis of the data collected through the questionnaire, the third step consisted in the development of a prototype of facial recognition for VLE. A total of 83 individuals, including students, face-to-face tutors, online tutors, coordinators, content teachers and research professors participated in the study. As a technological innovation for Online Education, our facial recognition prototype was implemented with the PHP and PYTHON languages, and the OPENCV computer vision library for haarcascade facial detection and facial recognition with Local Binary Histogram Patterns (LBPH). The tool was developed in order to recognize the student through facial patterns, recording their presence in Virtual Learning Environments. In the prototype tests, a database with 167 images was used, as well as the registration and recognition of 20 users and fraud simulation tests. For performance tests a database with 226 images was set up. The prototype demonstrated efficient performance and effective facial recognition of users, although it requires new implementations.

Keywords: Online Education; Virtual Learning Environment; Facial Recognition; Facial Biometry; Information Security.

LISTA DE FIGURAS

Figura 1: Face Interna: Imagem filtrada para extração somente da face interna na imagem capturada; Escala cinza: Imagem convertida em escala cinza; Equalizada: Imagem com o histograma equalizado.....	33
Figura 2: Histograma da imagem em escala cinza.....	34
Figura 3: Histograma equalizado da imagem.....	34
Figura 4: Classificadores disponibilizados pela ferramenta OPENCV.....	48
Figura 5: Exemplo dos formatos das características de Haar. 1 - Dois retângulos na vertical; 2 - Dois retângulos na horizontal; 3 - Três retângulos; 4 - Quatro retângulos.	50
Figura 6: Exemplo de Eigenface	52
Figura 7: Exemplo de Fisherface.....	53
Figura 8: Demonstração da Operação LBP.....	54
Figura 9: LBP Estendido	55
Figura 10: Ilustração da face com operadores LBP e o uso de histogramas	55
Figura 11: Exemplo de LPBH.....	56
Figura 12: Arquivos da função FACEDETECT do PHP	57
Figura 13: Resultado preliminar após executar o código feito em PHP para reconhecimento facial	58
Figura 14: Resultado após a edição simples da imagem.	59
Figura 15: Conjunto de imagens do Primeiro Indivíduo do Yale Face Database	63
Figura 16: Atributos dos Respondentes na EAD.....	64
Figura 17: Opinião dos respondentes sobre a possibilidade de fraude em AVAs.....	65
Figura 18: Respostas sobre a suficiência do método USUÁRIO/SENHA para ingresso nos AVAs	65
Figura 19: Respostas sobre a biometria para melhorar o monitoramento do estudante na EAD	66
Figura 20: Respostas sobre outros métodos biométricos nos AVAs.....	67
Figura 21: Respostas sobre a Biometria Facial na melhoria do monitoramento estudantil.....	67
Figura 22: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 2.....	72

Figura 23: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 4.....	72
Figura 24: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 7.....	73
Figura 25: Cenário de funcionamento do RECOFACE	77
Figura 26: Tela Inicial do RECOFACE	77
Figura 27: Tela Após efetuar o ingresso no RECOFACE.....	78
Figura 28: Arquitetura do protótipo.....	79
Figura 29: Enviando para o servidor as imagens para treinamento	80
Figura 30: Página de realização do Reconhecimento	81
Figura 31: Resultado do teste do algoritmo Python com o banco de imagens Yale Face Database	82
Figura 32: Resultado do código Python chamado pelo código PHP do RECOFACE.....	83
Figura 33: Exemplo de imagens salvas pelo RECOFACE com a nomeação adequada para o uso do código Python.....	84
Figura 34: Exemplo de imagens dos usuários capturadas pelo código em PHP e processada pelo código Python	85
Figura 35: Resultado do reconhecimento do usuário de identificação 5.	86

LISTA DE QUADROS

Quadro 1: Quadro comparativo do desempenho dos métodos biométricos.....	26
Quadro 2: Ferramentas similares que trabalham com Biometria	35

LISTA DE TABELAS

Tabela 1: Respondentes com experiência como tutor a distância	69
Tabela 2: Opinião dos tutores a distância sobre possibilidade de fraudes nos AVAs	70
Tabela 3: Suficiência do método Usuário/Senha segundo os Tutores a Distância ...	70
Tabela 4: Respostas dos tutores a distância sobre a viabilidade da biometria facial nos AVAs.....	71

LISTA DE SIGLAS E ABREVIATURAS

ASEE	<i>American Society for Engineering Education</i>
AVA	Ambiente Virtual de Aprendizagem
CERT.BR	Centro de Estudos, Resposta e Tratamento De Incidentes de Segurança No Brasil
EAD	Educação a Distância
E-LEARNING	Aprendizagem Eletrônica
GUI	Interface Gráfica do Usuário
IA	Inteligência Artificial
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
INTEL	<i>Integrated Electronics Corporation</i>
LBP	<i>Local Binary Patterns</i>
LDA	<i>Linear Discriminant Analysis</i>
MOODLE	<i>Modular Object-Oriented Dynamic Learning Environment</i>
OPENCV	<i>Open Source Computer Vision Library</i>
OPEN SOURCE	Software de Código Aberto
PCA	<i>Principal Component Analysis</i>
PHP	<i>Hypertext Preprocessor</i>
PROINFO	Programa Nacional de Tecnologia Educacional
XML	<i>Extensible Markup Language</i>

SUMÁRIO

1	INTRODUÇÃO	15
1.1	Justificativa do estudo	17
1.2	Problema de Pesquisa	18
1.3	OBJETIVOS	18
1.3.1	Geral.....	18
1.3.2	Específicos	18
1.4	Organização do Trabalho.....	19
2	AUTENTICAÇÃO DE ALUNOS NOS AMBIENTES VIRTUAIS DE APRENDIZAGEM.....	21
2.1	Segurança da Informação	21
2.2	Autenticação nos Ambientes Virtuais de Aprendizagem	23
2.3	Biometria	27
2.3.1	Reconhecimento facial	30
2.3.2	Processamento de imagens	31
2.4	FERRAMENTAS SIMILARES	35
2.4.1	Descrição das ferramentas.....	35
2.4.2	Comentários	38
3	METODOLOGIA	40
3.1	Tipo e natureza da pesquisa	40
3.1.1	Métodos de coleta e análise dos dados.....	41
3.2	Descrição da Pesquisa.....	42
3.3	Metodologia de Desenvolvimento do protótipo	43
3.3.1	Materiais e Métodos	45
3.4	OPENCV, PHP E PYTHON NA BIOMETRIA FACIAL	46
3.4.1	OPENCV	46
3.4.1.1	Bibliotecas do OPENCV.....	47
3.4.1.2	<i>Haarcascade</i>	48
3.4.1.3	Eigenface	51
3.4.1.4	Fisherface	52
3.4.1.5	Padrões binários locais de histogramas (LBPH).....	53
3.4.2	PHP	57
3.4.3	PYTHON.....	60

3.4.3.1	Hardware.....	61
3.4.3.2	Software	61
3.4.3.3	Banco de dados	62
4	RESULTADOS E DISCUSSÃO PRELIMINAR.....	64
4.1	Análise dos dados	73
5	RESULTADOS E DISCUSSÃO DO PROTÓTIPO (RECOFACE).....	76
5.1	Descrição do protótipo	76
5.2	Testes, Resultados e Análise.....	81
5.2.1	Testes do Protótipo.....	81
5.2.2	Resultados obtidos	84
5.2.3	Análise dos Resultados	87
6	CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS	89
	REFERÊNCIAS.....	91
	APÊNDICE A – QUESTIONÁRIO APLICADO NA PESQUISA	98
	APÊNDICE B – Códigos do protótipo.....	100

1 INTRODUÇÃO

O crescimento da Educação a Distância (EAD) no Brasil e a expansão do número de polos por todo o território nacional tem como exemplo característico a expansão que ocorreu no Instituto Federal do Piauí – IFPI, conforme Moraes (2015, p. 51) expõe:

A expansão territorial alcançada pela ampliação de polos de educação a distância e vagas no âmbito do Instituto Federal do Piauí é bastante significativa. Atualmente, o IFPI conta 69 (sessenta e nove) polos, e possui cerca de 12.208 (doze mil e duzentos e oito) alunos cadastrados no Sistema Nacional de Informações da Educação Profissional e Tecnológica (Sistec) referente até o ano de 2013. Recentemente esse número de alunos ampliou-se para 14.113 (quatorze mil e cento e treze) alunos cadastrados no Sistec, pois em 2014 foram ofertadas 1.900 (mil e novecentas vagas).

Segundo o Censo da Educação Superior (2013), no ano de 2012, 7.037.688 estudantes matricularam-se na Educação Superior, e destes alunos, 5.923.838 fizeram matrícula na educação presencial e 1.113.850, em cursos a distância. Os dados mostraram ainda que dos 1.113.850 matriculados na EAD, 181.624 matricularam-se em instituições públicas.

No mesmo sentido, Mello, C, Bergamo e Mello, R (2009, p. 135), concordam que “a demanda pela Educação a Distância cresce a cada dia para atender às exigências do mundo globalizado em mudanças aceleradas e com menor disponibilidade de tempo e espaços formais para educação.”

Segundo Abbad (2014), a EAD no Brasil é adotada em programas de qualificação e formação profissional, como também na educação corporativa, e na oferta de cursos para servidores públicos.

A EAD tem se tornado mais do que uma opção de ensino, mas sim, uma alternativa viável em termos econômicos, estruturais e de recursos humanos para os investimentos públicos e privados feitos na educação do nosso país. Segundo dados do Censo EAD 2012 (divulgado em 2013), o número de cursos na modalidade de educação a distância vem crescendo em larga escala. Bem como a maioria, em instituições privadas.

Nesse contexto, convém que a forte expansão seja acompanhada de uma preocupação com a qualidade do ensino, e, em particular, que sua execução seja

confiável e verificável. Esses são fatores importantes para que a Educação a Distância possa adquirir maior aceitação social no nosso país e no mundo globalizado.

Naturalmente, a rápida disseminação de novos recursos tecnológicos impulsionou as possibilidades de implantação e evolução da Educação a Distância:

A educação tem sido uma realidade na vida de muitas pessoas através da oferta de diversos cursos por todo o Brasil, possibilitando o crescimento do ensino superior nos locais mais inacessíveis do país. Com uma demanda de alunos interessados em uma nova forma de aprender, contando com recursos tecnológicos e rapidez na comunicação, tornou-se favorável a implantação da educação a distância (OLIVEIRA, 2016, p. 11,12).

No intuito de colaborar com melhorias tecnológicas, bem como com reflexões acerca de eficiência e confiabilidade no contexto da Educação a Distância, apresenta-se neste trabalho uma proposta de acesso aos Ambientes Virtuais de Aprendizagem (AVAs), em que se busca melhorias na Segurança da Informação através da autenticação dos alunos com a utilização da biometria facial. Além de uma alternativa de *login* na plataforma, entende-se essa proposta como uma ferramenta de acompanhamento ao aluno no decorrer do curso.

A pesquisa fundamenta-se na importância de se construir mecanismos tecnológicos para melhorar os processos da EAD, reforçando, para docentes e gestores, as garantias de autenticidade no acesso aos cursos e materiais didáticos disponibilizados nos AVAs. Logo, nesse estudo o fator primordial para a segurança dos Ambientes Virtuais de Aprendizagem será a identificação dos alunos na realização de um curso de ensino a distância (FIORESE; TAROUCO, 2006).

A biometria facial é o foco do nosso estudo. Para Pinheiro (2007), o uso da biometria é uma tendência na busca por autenticações mais seguras. Isso se deve ao fato dos meios biométricos não poderem ser perdidos ou esquecidos, e serem consideravelmente mais seguros e difíceis de serem copiados. Assim, postula-se que o uso de métodos biométricos na autenticação dos alunos proporciona uma melhoria na Segurança da Informação e no acompanhamento discente.

1.1 Justificativa do estudo

Conforme mencionado, a justificativa principal da pesquisa está relacionada com meios de garantir a autenticidade, no contexto da Educação a Distância, do aluno que ingressa em um Ambiente Virtual de Aprendizagem, contribuindo assim para o acompanhamento seguro de um curso por parte de docentes e gestores. Ou seja, nossa pesquisa propõe que métodos biométricos promovem o aumento da segurança nesses ambientes virtuais, fazendo com que somente pessoas autorizadas acessem e enviem informações para o sistema. Trata-se então de uma contribuição para dois quesitos sensíveis no processo de implantação da Educação a Distância: a confiabilidade e a qualidade dessa modalidade de ensino.

Dessa forma, baseados na importância de mecanismos biométricos para a segurança da informação e na importância do desenvolvimento de tecnologias voltadas para autenticação de alunos nas ferramentas de Educação a Distância, propõe-se um protótipo de reconhecimento facial compatível com a Educação a Distância, que aliado ao mecanismo de autenticação usuário e senha, traz como contribuição prover maior segurança nos AVAs. Segundo Penteado (2009), a autenticação baseada em senhas ainda é predominante.

Ademais, a solução de identificação biométrica via reconhecimento facial tem boas possibilidades de implementação em larga escala, em razão da popularização do *hardware* necessário. Penteado (2009, p. 2) relata que,

Com a popularização e conseqüente barateamento dos preços de hardware habilitado para a aquisição de dados biométricos (webcams, microfones, leitores de impressões digitais), assim como a popularização do acesso à Internet de banda larga, a Biometria torna-se uma forma viável de autenticação remota de indivíduos em aplicações Web.

Com a autenticação por meio de reconhecimento facial, o controle de acesso é mais rígido, o que garante que a participação dos alunos seja mais confiável, e traz benefícios tanto para o Corpo Discente, quanto para o Corpo Docente. Portanto, contribuindo com mecanismos tecnológicos para a instituição de ensino.

1.2 Problema de Pesquisa

O presente estudo busca obter uma solução de Segurança da Informação para os Ambientes Virtuais de Aprendizagem, a partir de um estudo sobre como a biometria facial pode contribuir para a melhoria dos dados trafegados nas plataformas de ensino. Atualmente, várias formas de autenticação são utilizadas comercialmente, porém a Educação a Distância é influenciada por fatores de ordem econômica.

Dessa forma, coloca-se a seguinte pergunta: *a Biometria Facial pode contribuir com a Segurança da Informação dos Ambientes Virtuais de Aprendizagem (AVA) no monitoramento e acompanhamento dos alunos da Educação a Distância?* A fim de responder esse questionamento, nossa pesquisa faz uma avaliação dos mecanismos utilizados para autenticar os alunos nas plataformas de estudos, e argumenta sobre as vantagens da Biometria Facial como alternativa eficiente e viável (simples e de baixo custo) de monitoramento estudantil para essa modalidade de ensino, facultando acompanhar a participação do estudante nas diversas atividades disponibilizadas no ambiente.

Para tanto, pesquisou-se a opinião de profissionais envolvidos na Educação a Distância sobre a perspectiva de controle biométrico no AVA. Realizou-se um estudo sobre a implementação de uma ferramenta de identificação biométrica chamada RECOFACE, no AVA Moodle, em que foram realizados testes, a fim de justificar sua importância dentro do cenário educativo e obter conhecimento sobre a exploração desse conceito na Educação a Distância.

1.3 OBJETIVOS

1.3.1 Geral

Desenvolver um protótipo de autenticação biométrica facial que possa ser integrado em Ambientes Virtuais de Aprendizagem, com o propósito de contribuir com a Segurança da Informação dos cursos da Educação a Distância.

1.3.2 Específicos

- Investigar ferramentas similares de autenticação biométricas e biométricas faciais utilizadas em Ambientes Virtuais de Aprendizagem.

- Investigar a percepção de integrantes da EAD do Instituto Federal do Piauí e da Universidade Federal do Piauí acerca do uso da autenticação biométrica facial em Ambientes Virtuais de Aprendizagem.
- Demonstrar como a Biometria Facial pode contribuir com a Segurança da Informação nos Ambiente Virtuais de Aprendizagem utilizados em cursos na modalidade de Educação a Distância (EAD).

1.4 Organização do Trabalho

Este trabalho está organizado da seguinte forma:

1. **Introdução:** Apresenta uma introdução sobre a Educação a Distância e os Ambientes Virtuais de Aprendizagem, apresentando o problema da pesquisa, justificativas que motivaram a realização da mesma e seus objetivos.
2. **Autenticação de alunos nos Ambientes Virtuais de Aprendizagem:** Esse capítulo faz uma abordagem teórica sobre a Segurança da Informação nos Ambientes Virtuais de Aprendizagem, apresentando diferentes formas de autenticação biométrica.
3. **Metodologia:** Descreve os passos realizados na construção da pesquisa, os métodos e materiais utilizados para levantamento dos requisitos do protótipo; além disso, descreve os procedimentos metodológicos de desenvolvimento do protótipo.
4. **Resultados e discussão preliminar:** Nesse capítulo são abordados os resultados encontrados no questionário aplicado na pesquisa, discutindo as informações encontradas na coleta dos dados.
5. **Resultados e discussão do protótipo (RECOFACE):** Nesse capítulo temos a descrição do produto – o módulo RECOFE para reconhecimento facial nos AVAs – das tecnologias utilizadas na sua implementação, a descrição do seu funcionamento, a forma de implementação, testes realizados, resultados obtidos e análise dos resultados.

6. **Considerações finais e trabalhos futuros:** Nesse capítulo são apresentadas as considerações feitas sobre o trabalho de pesquisa, listando trabalhos futuros a serem realizados para a melhoria do protótipo.

Por fim, apresentamos as referências bibliográficas e os apêndices.

Apêndice A: Apresenta o questionário aplicado na pesquisa.

Apêndice B: Apresenta os códigos do protótipo.

2 AUTENTICAÇÃO DE ALUNOS NOS AMBIENTES VIRTUAIS DE APRENDIZAGEM

É evidente que a informação é um recurso essencial para a vida das organizações e das instituições. Por isso, é necessário tê-la sob controle e segurança, o que requer investimentos em novas formas e tecnologias para se obter esse controle. Esse fato se aplica em particular no contexto da Educação.

O presente capítulo faz uma abordagem teórica sobre Segurança da Informação nos Ambientes Virtuais de Aprendizagem, apresentando diferentes formas de autenticação biométrica, explorando especificamente a biometria facial, o reconhecimento facial, o processamento de imagens e discutindo algumas ferramentas que fazem uso da biometria.

2.1 Segurança da Informação

Atualmente os avanços das ferramentas tecnológicas proporcionam benefícios diversos e inovam nas modalidades de negócios. São exemplos: *e-commerce*, bancos *on-line*, armazenamento na nuvem, ensino a distância, entre outros. Esses avanços trazem consigo novos riscos à Segurança da Informação e aos dados da empresa e dos clientes, que podem gerar prejuízos em uma situação de acesso não autorizado. Esses prejuízos podem ser financeiros, conceituais e intelectuais.

Ramos (2006) define a segurança da informação como a forma de proteger os ativos da informação, mais especificamente, aqueles que produzem, processam, transmitem ou armazenam informações.

Para Nakamura e Geus (2010) a Segurança da Informação não deve envolver somente a proteção contra intrusos, *hackers*, maus funcionários ou vírus. Para que se possa melhorar a segurança de uma plataforma, é necessário estabelecer normas de segurança. Para que um ataque seja bem-sucedido, diversos fatores são levados em consideração, como a obtenção de dados sobre o alvo e suas vulnerabilidades, saber explorar essas vulnerabilidades e saber como apagar os seus rastros após o ataque. Castanha (2014) descreve práticas para a obtenção de acesso a informações importantes ou sigilosas por meio da exploração dos recursos humanos dentro das organizações. Para realizar essas práticas, o indivíduo que quer explorar as

vulnerabilidades de um sistema pode se passar por outra pessoa, ou fazer a utilização de outras técnicas. Castanha (2014) chama essas práticas de “Engenharia Social”.

Segundo Giavaroto e Santos (2013, p.36):

Não existe correção para vulnerabilidades envolvendo o fator humano, porém, é possível diminuir a ação de engenheiros sociais através de treinamentos constantes de conscientização de todo o pessoal envolvido nos processos.

Sendo assim, o fator especificamente humano é crucial para as vulnerabilidades dos Sistemas de Informação, e depende muito da conscientização por parte dos componentes que possuem acesso ao sistema, ou que são beneficiados por ele. Mas o desenvolvimento de novas ferramentas tecnológicas que restrinjam a vulnerabilidade também pode contribuir com esse processo: nos conceitos básicos de Segurança da Informação, a segurança deve envolver diversos aspectos, dentre eles, humanos, tecnológicos, jurídicos, de negócios e processuais. Segundo Nunan, Costa Filho e Lima (2016, p. 113), a Segurança da Informação “é alcançada a partir de um conjunto de instrumentos que englobam políticas, processos, procedimentos, estruturas organizacionais, *software* e *hardware*, em conjunto com outros processos da gestão da informação”. Segundo Nakamura e Geus (2010), convém fazer com que a Segurança da Informação, na sua globalidade, seja bastante elaborada, e que todos os cuidados sejam tomados para garantir a segurança de um sistema.

Para Nakamura e Geus (2010) a segurança significa lucro para as organizações, e resulta em flexibilidade, facilidade e disponibilidade dos recursos de informática. Nesse contexto, a Segurança da Informação tem um real valor na sobrevivência das organizações, em que os sistemas que oferecem seus serviços com maior segurança serão aqueles que granjearão maior confiabilidade entre seus utilizadores. Nessa linha, a segurança da informação possibilita a melhoria da confiabilidade na modalidade EAD.

Nos sistemas voltados para educação *on-line*, a segurança deve ser quesito de destaque da mesma forma que em outros sistemas empresariais. Com isso, é necessário o incentivo aos estudos relacionados com essa área de investigação, possibilitando melhorias na segurança nos Ambientes Virtuais de Aprendizagem. Segundo Nakamura e Geus (2010) “Um atacante precisa encontrar somente uma brecha para realizar um ataque, enquanto o gestor de segurança deve conhecer

todas as brechas e fecha-las”. Essa é uma filosofia principal na elaboração da segurança nos diversos níveis dos Sistemas de Informação, e em se tratando da EAD, implica que devemos agregar alternativas na autenticação nessas plataformas.

Em se tratando de *acesso*, este é mais comumente feito através do fornecimento de credenciais de usuário e senha. Após a identificação do usuário, deve-se proceder à sua *autenticação*, isto é, o programa deve confirmar se o usuário é realmente quem ele diz ser. Os sistemas trabalham de forma a autenticar com uma combinação de *hardware*, *software* e seus processos que dão o acesso aos usuários e aos recursos computacionais diversos. Mas já existem sistemas modernos utilizando cartões inteligentes, *tokens* que geram senhas para acesso, ou outros tipos de métodos de acesso (FIORESE, 2000; BERNARDI, 2007). Sistemas mais robustos e sofisticados, aliados a dispositivos de *hardware*, podem trabalhar com a autenticação através de características físicas. Essas características podem ser: o formato da mão, da retina ou do rosto, impressão digital, reconhecimento de voz e facial.

Na próxima seção, abordaremos a autenticação nos AVAs, problema principal atacado em nossa pesquisa.

2.2 Autenticação nos Ambientes Virtuais de Aprendizagem

A autenticação é o processo pelo qual o sistema verifica se o requisitante remoto é realmente quem ele diz ser (BRAGA, 2013). É essencial para controlar o acesso aos diversos tipos de Sistemas de Informação presentes na Educação a Distância. O processo de autenticação pode permitir a realização de auditorias no sistema, para que se possa realizar o monitoramento e prevenção de fraudes.

Basicamente há três métodos gerais para autenticação:

- Identificação Positiva ou aquilo que o usuário sabe: É a autenticação na qual o usuário demonstra conhecimento de alguma informação que gere a autenticação. Exemplo: *E-mail* e Senha.
- Identificação Proprietária ou aquilo que o usuário tenha: É a autenticação feita através de algo que o usuário tenha especificamente para o processo de ingresso. Exemplo: Cartão Magnético.

- Identificação Biométrica ou aquilo que o usuário é: É a autenticação que utiliza uma característica biológica individual e específica do usuário. Exemplo: A impressão digital.

Uma fraqueza dos dois primeiros tipos de autenticação é o fato de poderem ser copiados, esquecidos, armazenados de forma insegura, roubados, furtados ou usados por pessoas não autorizadas. Os sistemas biométricos são uma das formas de aumentar a segurança da informação, proporcionando maior fidelidade na autenticação. A esse respeito, Furlano Neto e Bellinetti (2005) relatam que em 2004 ocorreu um aumento de 34% na quantidade de ataques a computadores de empresas, o que representa um prejuízo em torno de 400 milhões de reais. Segundo o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) (2015), em 2015 houve o quantitativo de 722.205 incidentes reportados, sendo que 168.775 foram tentativas de fraudes. O CERT.br (2015) relata também que uma grande quantidade desses ataques ocorre através da exploração do método usuário e senha. Portanto, “Atualmente a biometria está sendo utilizada em diversos setores, desde reconhecimento de indivíduos na área de segurança até transações financeiras em grandes corporações bancárias” (BERNARDI, 2007, p. 41).

Silva (2016, p. 2) define um Ambiente Virtual de Aprendizagem como “uma plataforma on-line que agrega diferentes aplicações que permitem armazenar, disponibilizar e administrar a interação entre os atores (professores, alunos, tutores, equipe técnica, etc.) envolvidos no processo de ensino-aprendizagem.” Para se ter acesso ao AVA, os participantes desse processo devem realizar uma autenticação.

Ademais, sabemos que na Educação a Distância os atores do processo possuem papéis distintos, e recebem também papéis distintos dentro das plataformas. Ou seja, nas ferramentas *e-learning*, os tutores possuem uma forma de acesso e uma forma específica de permissão, assim como os coordenadores e alunos possuem os seus níveis de permissão e acesso.

A autenticação nos AVAs é especialmente importante nos momentos avaliativos (FIORESE, 2000), pois contribui para garantir a identidade do aluno que está realizando a avaliação (BERNARDI, 2007). Portanto, a melhoria dos processos de Segurança da Informação nos AVAs pode contribuir com a melhoria da formação do estudante no contexto da Educação a Distância. De fato, o acompanhamento tanto no *login*, quanto no andamento das atividades, é uma forma de motivar o aluno a estar

presente desde o início de seus estudos, até a conclusão das suas atividades (ROLIM, 2009). O descuido com o processo de autenticação aumenta a vulnerabilidade do sistema, não só no que se refere ao acesso ao conteúdo da disciplina, mas também na garantia da participação do aluno nas atividades do curso. Isso ocorre pela facilidade de substituição do aluno que deveria ser avaliado por outra pessoa (RABUZIN; BACA; SAJKO, 2006).

Refletindo acerca dessa questão,

A maioria dos AVAs não dispõe de recursos eficientes e automatizados que garantam a participação dos usuários no desenvolvimento de suas atividades acadêmicas, incluindo seu processo de avaliação via Internet. (RABUZIN; BACA; SAJKO, 2006 apud DINIZ, 2013a, p. 17).

O acesso aos AVAs na maioria das vezes é feito através de informações que o aluno conhece. Essas informações podem ser um nome de usuário e uma senha. Porém, na maioria dos AVAs esse tipo de acesso não resulta em uma segurança adequada (BERNARDI, 2007), uma vez que,

O uso deste tipo simples de autenticação aumenta a vulnerabilidade a fraudes, tanto no acesso ao sistema quanto durante a participação do aluno nas atividades e nas avaliações do curso, pois outra pessoa pode substituir facilmente o indivíduo que deveria ser avaliado no AVA. (RABUZIN; BACA; SAJKO, 2006 apud DINIZ, 2013a, p.17).

Existem várias soluções para identificar os usuários em aplicações comerciais (MARAIS et al., 2006). Porém, nos AVAs abertos essas técnicas não são utilizadas devido a restrições econômicas (MARAIS et al., 2006). Uma alternativa é discutida por Rolim e Bezerra (2008), que apresentam uma solução de identificação da face para ser usado em um AVA através do uso da *webcam*. A ferramenta possui arquitetura cliente-servidor. Essa solução trabalha com a segurança digital na identificação de alunos online no AVA e será detalhada na seção 2.4.

No Quadro 1, é apresentado um quadro comparativo das formas biométricas de acesso, seus aspectos de vantagens e desvantagens. Uma descrição dos aspectos abordados pode ser encontrada em Jain, Ross e Prabhakar (2004):

- **Universalidade:** Significa que todas as pessoas possuem a característica.

- **Distinção:** Indica a diferenciação dessas características entre as pessoas.
- **Permanência:** Indica que as características não devem variar durante o tempo.
- **Mensuração:** Indica a capacidade de se medir quantitativamente.
- **Desempenho:** Indica a precisão na identificação.
- **Aceitabilidade:** Refere-se à aceitação das pessoas sobre o método.
- **Circunvenção:** Refere-se à possibilidade de o método ser enganado.

Quadro 1: Quadro comparativo do desempenho dos métodos biométricos.

Identificador Biométrico	Universalidade	Distinção	Permanência	Mensuração	Desempenho	Aceitabilidade	Circunvenção
DNA	Alta	Alta	Alta	Baixa	Alta	Baixa	Baixa
Orelha	Média	Média	Média	Média	Média	Alta	Média
Termograma da Face	Alta	Alta	Baixa	Alta	Média	Alta	Baixa
Impressão Digital	Média	Alta	Alta	Média	Alta	Média	Média
Marcha	Média	Baixa	Baixa	Alta	Baixa	Alta	Média
Geometria da Mão	Média	Média	Média	Alta	Média	Média	Média
Veias da Mão	Média	Média	Média	Média	Média	Média	Baixa
Íris	Alta	Alta	Alta	Média	Alta	Baixa	Baixa
Teclar	Baixa	Baixa	Baixa	Média	Baixa	Média	Média
Odor	Alta	Alta	Alta	Baixa	Baixa	Média	Baixa
Impressão da Mão	Média	Alta	Alta	Média	Média	Média	Média
Retina	Alta	Alta	Média	Baixa	Média	Média	Média
Assinatura	Baixa	Baixa	Baixa	Alta	Baixa	Alta	Alta
Voz	Média	Baixa	Baixa	Média	Baixa	Alta	Alta
Face	Alta	Baixa	Média	Alta	Baixa	Alta	Alta

Fonte: JAIN K. A.; ROSS, A.; PRABHAKAR, S. (2004)

Conforme apresentado no Quadro 1, o método biométrico facial apresenta vantagens e desvantagens. Mas julgamos que suas características a tornam elegível para nossos objetivos, em particular devido à sua aceitabilidade como método de autenticação. Por exemplo, os dispositivos de captura operam de forma não invasiva, são de baixo custo e de fácil utilização. Além disso, os métodos de reconhecimento facial possuem algoritmos sofisticados que aliados à evolução do *hardware*, demonstram um desempenho aceitável (MORAES, 2010). Diniz et al (2013b), confirma que a autenticação biométrica facial obteve uma taxa de reconhecimento de 92%, com a utilização da técnica K-NN, PCA e *Eigenfaces*.

Com isso, defendemos que a autenticação nos AVAs pode envolver também a verificação de características físicas, e escolhemos a biometria facial para ser explorada como método de autenticação nos AVAs.

2.3 Biometria

A palavra Biometria é composta de dois elementos gregos: *bios* = vida e *metron* = medida. Portanto, daí tem-se a medida dos seres vivos, ou seja, mensuração dos seres vivos. Segundo Kazienko (2003), a Biometria é a disciplina científica que estuda as características físicas dos seres vivos, abordando-as de forma estatística, e analisando seus padrões, definindo-os em atributos quantitativos. Distância entre os olhos, impressões digitais, formas e cores na íris e a formação das veias são algumas das características físicas que tornam cada ser humano único (o mesmo valendo para outros seres vivos), tornando possível desenvolver aplicações e técnicas para reconhecimento e identificação desses padrões (CASTILHO, 2012).

Além das características físicas, as comportamentais são também relevantes para fins de identificação biométrica, de forma que podemos classificar as características de interesse na Biometria como:

- **Físicas:** retina, íris, geometria da palma da mão, formato da unha, a face e a impressão digital;
- **Comportamentais:** assinatura manuscrita, voz, maneira de andar, entre outras.

As técnicas de Biometria na atualidade são amplamente estudadas e utilizadas, e dentre seus usos destaca-se a segurança, pois as mesmas possibilitam um controle de acesso adequado a sistemas e locais. Esse controle pode envolver desde usuários

num computador pessoal acessando a Internet, por exemplo para abrir seu Sistema Operacional, até em grandes corporações que possuem locais de acesso restrito, ou mesmo a identificação de criminosos (PATIN, 2007).

A simplicidade para o reconhecimento de pessoas é um dos fatores da popularização da Biometria. E em situações que necessitam autenticação, pode ser a escolha mais indicada: mecanismos como cartões, senhas e chaves podem ser perdidos, clonados, roubados ou emprestados, enquanto que os dados biométricos são características do indivíduo. Para Almeida (2003), a progressão das tecnologias biométricas, aliada à redução dos custos dos equipamentos, fez com que surgissem novas pesquisas sobre Biometria em ambientes *web*. Através de algoritmos aplicados no desenvolvimento de *software*, é possível fazer um reconhecimento rápido e confiável utilizando a leitura e armazenamento seguro dos dados.

Em particular, o reconhecimento de faces é uma tarefa realizada com naturalidade pelo ser humano, pois possui fácil abstração. Com isso, vários pesquisadores se interessaram pela face na identificação biométrica, além da possibilidade da realização dessa tarefa por computadores de forma eficaz. Segundo Sung e Poggio (1994), identificação de faces é a determinação da existência ou não de um rosto na imagem e uma vez encontrado este objeto, sua localização deve ser apontada através de um enquadramento ou obtendo as suas coordenadas dentro da imagem disponibilizada, de forma a quantificá-la matematicamente.

Por outro lado, não é uma tarefa fácil criar um padrão para o reconhecimento da face. Os rostos humanos dispõem de estruturas semelhantes como boca, nariz, olhos, entre outras, que são dispostas nas mesmas configurações de espaço, com texturas diferentes, cores variadas, presença de outras características como barba e uma quantidade considerável de componentes que influenciam essa detecção, como por exemplo, nariz mais avantajado ou menos avantajado; lábios menos carnudos ou mais carnudos, etc. Além disso, os rostos normalmente utilizam adornos ou enfeites, como óculos ou bigodes, que podem estar ausentes ou presentes (quando presentes podem ocultar características básicas da face).

Ademais, pode ser mais difícil identificar as condições dos rostos em lugares com pouca ou muita iluminação, sendo esse um fator discriminante na detecção. Objetos e cores de fundo também influenciam, pois podem esconder ou criar sombras no rosto. Isso é devido ao formato tridimensional da face. Dessa forma, a Biometria

facial depende do desenvolvimento de algoritmos sofisticados, conforme discutimos mais abaixo.

No quesito Segurança da Informação, a Biometria facial tem vantagens que já foram descritas no presente trabalho. Essas vantagens são potencializadas à medida que a Educação a Distância necessita de formas de garantir a qualidade de ensino. Essa qualidade está ligada diretamente com a comprovação do tempo de estudo que o aluno perfaz na plataforma, o que influencia diretamente no aproveitamento qualitativo e quantitativo desse estudante em relação aos conteúdos ministrados nas disciplinas e no curso do qual o mesmo participa.

No quesito viabilidade, cabe mencionar que os dispositivos tecnológicos comercializados atualmente, de maneira uniforme, dispõem de câmeras digitais que possuem uma qualidade adequada para a Biometria da face. Com os incentivos governamentais dos últimos anos, houve uma uniformização do acesso aos dispositivos que apresentam configurações modernas, através da diminuição da carga de impostos sobre esses produtos. Em 2005, o Governo Federal lançou por meio do decreto 5.602 de 6 de Dezembro de 2005, a redução de cargas tributárias sobre os equipamentos tecnológicos comercializados no varejo. Isso ocorreu para estimular a inclusão digital e social (BRASIL, 2005). Dentre outros programas, o ProInfo foi um deles e tinha como objetivo específico “Contribuir com a inclusão digital por meio da ampliação do acesso a computadores, da conexão à rede mundial de computadores e de outras tecnologias digitais, beneficiando a comunidade escolar e a população próxima às escolas” (BRASIL, 2007). Nessa linha, Martins e Lucas (2012) citam outros programas governamentais de inclusão digital: Casa Brasil, o programa Governo Eletrônico Serviço de Atendimento ao Cidadão (GESAC), Maré – Telecentros de Pesca, Projeto Cidadão Conectado: computador para todos, Programa Computadores para a inclusão, Programa Computador portátil para professores, entre outros.

Um aspecto frágil do reconhecimento facial advém da possibilidade de mudanças físicas que os indivíduos sofrem ao longo do tempo. Porém, esse aspecto não é um impedimento para o uso na EAD, visto que os cursos duram tempo limitado, e os alunos podem solicitar alterações nas credenciais.

Na sequência, discutimos brevemente sobre reconhecimento facial e processamento de imagens, temas centrais em nossa pesquisa.

2.3.1 Reconhecimento facial

O reconhecimento facial é uma das formas de Biometria que desperta maior interesse para a pesquisa científica.

Castilho (2012, p. 25) relata que:

Denomina-se reconhecimento facial em processamento de sinais a processos automatizados ou semi-automatizados que através de técnicas matemáticas comparam imagens faciais de entrada com imagens faciais armazenadas em um banco de dados e determinam se tais imagens testadas fazem parte ou não do banco de dados, e se fizerem, indicam qual é essa imagem.

Segundo Pereira (2007), a maioria das ferramentas de *software* de reconhecimento facial que estão e vêm sendo desenvolvidas baseiam-se em certos pontos característicos e estratégicos da face, como a distância entre os olhos, a profundidade dos olhos, o tamanho do nariz, a linha do queixo, a distância entre os olhos e sobrancelha, entre outros pontos que dependendo do desenvolvedor, podem ser aproveitados. A correta identificação e captura desses pontos pode ser feita em uma imagem com duas dimensões apenas, mapeando os pontos a serem analisados e construir um modo de adaptá-la em três dimensões geométricas, com a finalidade de obter maior precisão.

Logo após tirar a fotografia, uma transformação é feita em cada ponto para dados numéricos que serão comparados a outros que estejam contidos em um banco de dados.

Segundo Pereira (2007), várias formas de reconhecimento desses padrões podem ser levadas em consideração, como o reconhecimento em imagens faciais que não sejam imagens frontais, reconhecimento em ambiente externo que receba influência de luzes, reconhecimento de faces masculinas, que são mais propícias ao reconhecimento por terem características mais acentuadas, e de mulheres, que têm características na maioria das vezes suavizadas e que dificultam o reconhecimento.

Pereira (2007) também diz: “O reconhecimento facial através de imagens em duas dimensões leva em conta diversos padrões apresentados na face da determinada pessoa, como as medidas e proporções faciais”. Através desses dados, podemos processar a imagem visando obter informações acerca do padrão facial do estudante. Pode-se obter a distância dos olhos, dos olhos para a boca, da boca para

o nariz. Com isso, podemos armazenar esses dados em um Banco de Dados e deixá-los registrados para futuras consultas.

Os métodos de Biometria Facial utilizam técnicas de *aprendizagem computacional*. Esse recurso é similar à percepção do ser humano para reconhecer padrões, porém é necessário “treinar” a máquina para o reconhecimento (PEREIRA, 2007). Quanto maior a proximidade do indivíduo humano com outros, maior a capacidade de identificar a sua face e o seu padrão facial. O cérebro “aprende” a identificar esses padrões. Através dessa percepção, chegou-se à conclusão que se uma máquina fosse submetida à análise de grandes quantidades de dados repetidas vezes, ela poderia simular a inteligência humana através do uso de algoritmos complexos e específicos para esse uso. *Redes Neurais* são um formalismo tradicional para uso em aprendizagem de máquina.

Nessa direção,

Um processo de aprendizagem inclui a aquisição de novas formas de conhecimento: o desenvolvimento motor e a habilidade cognitiva (através de instruções ou prática), a organização do novo conhecimento (representações efetivas) e as descobertas de novos fatos e teorias através da observação e experimentação. Desde o início da era dos computadores, tem sido realizadas pesquisas para implantar algumas destas capacidades em computadores. Resolver este problema tem sido o maior desafio para os pesquisadores de inteligência artificial (IA). O estudo e a modelagem de processos de aprendizagem em computadores e suas múltiplas manifestações constituem o objetivo principal do estudo de aprendizado de máquinas. (SANTOS, 2005, p. 10).

Na sequência, discutimos um conteúdo mínimo de processamento de imagens para uso em reconhecimento facial.

2.3.2 Processamento de imagens

Esta seção apresenta um mínimo de conceitos de processamento de imagens envolvidos em nossa pesquisa. Uma exposição aprofundada do tema pode ser encontrada no livro “Processamento Digital de Imagens”, dos autores Rafael C. Gonzalez e Richard E. Woods.

Uma imagem digital pode ser expressa como uma função $f(x,y)$, sendo representada como uma matriz cujos índices de linhas e de colunas identificam os pontos na imagem. Os elementos dessa matriz digital são conhecidos pela palavra

"pixels" (FIGUEREDO, 2011). O valor de f nos pares ordenados (x, y) é chamado de nível de cinza, em uma imagem monocromática, da imagem no determinado ponto (GONZALEZ; WOODS; EDDINS, 2009 apud CORDEIRO, 2015). Nesse contexto, Gonzalez; Woods; Eddins, (2009 apud Cordeiro 2015, p. 38), define que "o pixel é o menor elemento que compõe uma imagem digital, e ele possui um valor de intensidade. Cada pixel possui uma cor, representado em um ponto da imagem."

O processamento de imagens diz respeito às operações matemáticas sobre dados de um arquivo de imagem, visando a sua transformação em uma imagem de melhor qualidade espectral e espacial para uma finalidade específica (MENEZES, 2012). Nesse sentido,

A finalidade principal do processamento de imagens é o aprimoramento de informações pictóricas para interpretação humana ou a análise automática por computador de informações extraídas de uma cena. É caracterizado por soluções específicas, pois técnicas que funcionam bem para determinado problema podem mostrar-se inadequadas para outros. (CASTILHO, 2012, p. 23).

Para que o reconhecimento facial seja possibilitado, é preciso realizar um tratamento nas imagens estáticas, uma série de procedimentos de preparação que envolvem técnicas de processamento de imagens. Um dos cuidados a serem trabalhados é o tratamento da parte externa à face presente na imagem. Outros cuidados são: a correção de iluminação; o tratamento digital para melhoramento da imagem; a forma de aquisição de imagem; a extração dos objetos do fundo; a parametrização da imagem, definindo a área do objeto a ser analisado; o reconhecimento dos objetos a serem realizados através de ferramentas específicas.

Dessa forma, os principais métodos que são utilizados para adequar a imagem para reconhecimento de padrões são: a conversão da imagem de colorido para tons de cinza, a binarização (adequação da imagem para diferenciar as tonalidades de cores e poder separar um fundo de uma face), a detecção dos contornos, e a segmentação da imagem (dividir a imagens em regiões para facilitar a análise de seus contornos). (CASTILHO, 2012).

O processo executado na imagem tem o objetivo de facilitar a análise pelo computador através dos algoritmos utilizados. O cenário onde a fotografia foi retirada influencia muito no resultado dessa análise, e deve ser escolhido de forma adequada, com a finalidade de melhorar o processamento da imagem.

Na implementação deste trabalho, foram aplicadas algumas técnicas de processamento de imagens visando preparar os retratos dos usuários para um melhor desempenho do sistema na identificação. O processamento realizado consiste em redimensionar a imagem, converter as imagens coloridas capturadas para escala cinza, aplicar o *método de Viola e Jones* (VIOLA; JONES, 2001; VIOLA; JONES, 2004) para obter somente a face na imagem, e equalizar o histograma (o conceito de histograma é abordado em seguida).

Histogramas de uma imagem digital são técnicas utilizadas no processamento de imagens no domínio do espaço. O histograma é útil para obter estatísticas ou realçar uma imagem, indicando qualitativamente o nível de brilho e contraste de uma imagem (GONZALEZ; WOODS; EDDINS, 2009 apud CORDEIRO, 2015).

Desta forma, a equalização do histograma tem como objetivo obter um histograma uniforme de uma imagem, com alto contraste, facilitando a identificação de elementos em uma imagem inicial (GONZALEZ; WOODS; EDDINS, 2009 apud CORDEIRO, 2015).

Nessa direção, “A equalização do histograma consiste em ajustar a escala de tons de cinza de uma imagem para que os níveis de tons de cinza da imagem de entrada seja mapeada em um histograma uniforme” Gonzalez; Woods; Eddins, (2009 apud Cordeiro, 2015, p. 40).

Em seu trabalho, Castilho (2012) ilustra o processo realizado para segmentação da face, convertendo para níveis de cinza e a imagem após a equalização de histograma. A ilustração está presente na Figura 1.

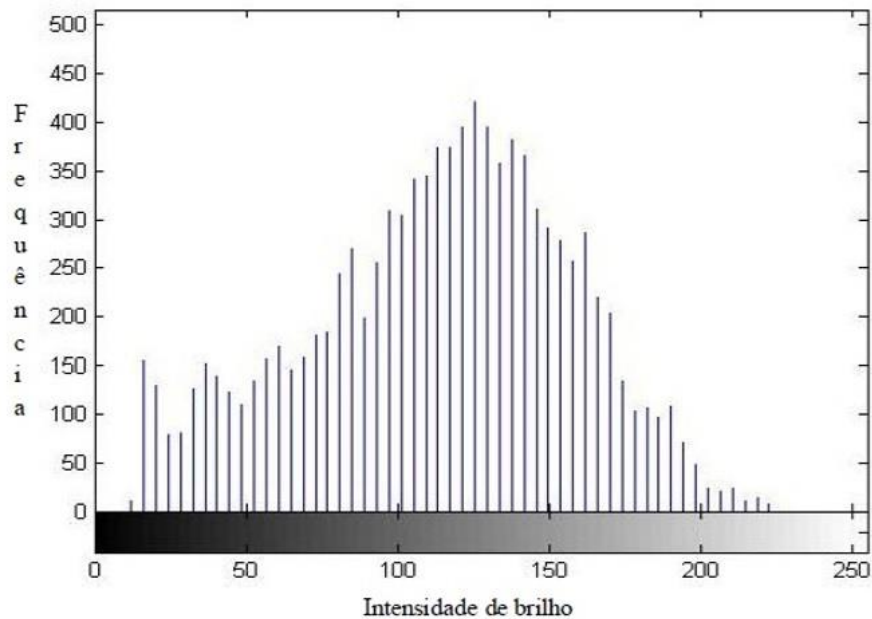
Figura 1: Face Interna: Imagem filtrada para extração somente da face interna na imagem capturada; Escala cinza: Imagem convertida em escala cinza; Equalizada: Imagem com o histograma equalizado.



Fonte: CASTILHO J. M. (2012)

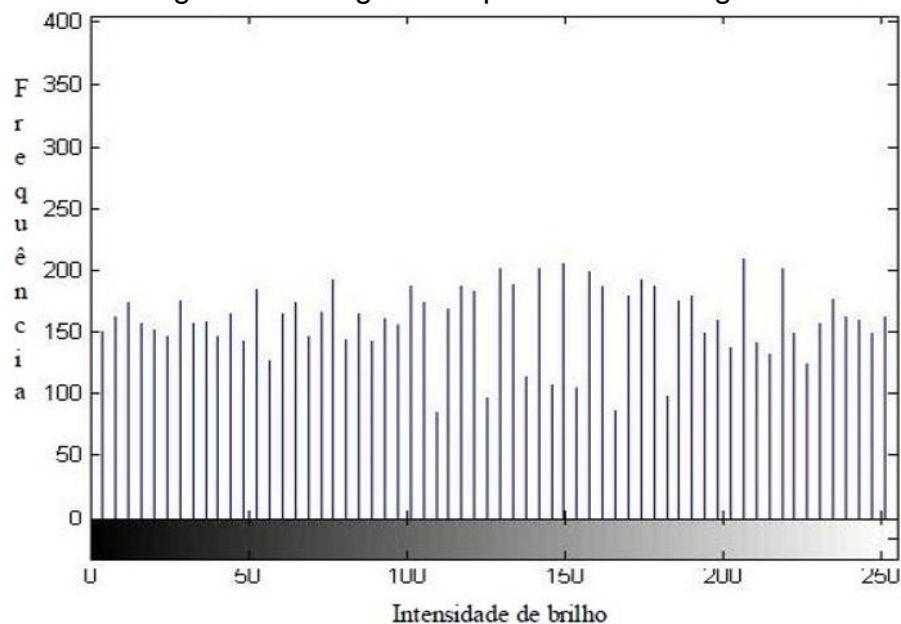
Castilho (2012) também reforça a necessidade de equalizar o brilho e o contraste da imagem, equalizando-a. O método é utilizado para padronizar o brilho e o contraste das imagens. O objetivo desse método é preparar as imagens para um melhor desempenho do protótipo. Na figura 2 (ilustra o histograma da imagem em escala cinza) e figura 3 (o histograma da imagem equalizado) podemos observar a equalização em histograma da imagem.

Figura 2: Histograma da imagem em escala cinza.



Fonte: CASTILHO J. M. (2012)

Figura 3: Histograma equalizado da imagem.



Fonte: CASTILHO J. M. (2012)

2.4 FERRAMENTAS SIMILARES

2.4.1 Descrição das ferramentas

Como parte integrante da pesquisa bibliográfica, realizamos um levantamento de outros trabalhos apresentando soluções similares, abordando não somente ferramentas da biometria facial, mas também ferramentas biométricas de forma geral, no contexto de Ambientes Virtuais de Aprendizagem. Esse levantamento está sumarizado no Quadro 2.

Quadro 2: Ferramentas similares que trabalham com Biometria

	BIOAUTH¹	BIOSIG-ID²	FACEID³
MERCADO DE ATUAÇÃO	EDUCACIONAL (MOODLE)	PODE SER UTILIZADO NA EDUCAÇÃO, PÓREM NÃO É FEITO PARA A EDUCAÇÃO	VÁRIOS MERCADOS QUE POSSAM UTILIZA-LO VIA WEB
TÉCNICA DE FUNCIONAMENTO	TRABALHA NOS QUESTIONÁRIOS OU ONDE O ALUNO NECESSITE DIGITAR.	IDENTIFICA O COMPORTAMENTO NO DESENHO	IDENTIFICA A FACE ATRAVÉS DE UM SERVIÇO WEB
BIOMETRIA	BIOMETRIA COMPORTAMENTAL POR DIGITAÇÃO	BIOMETRIA COMPORTAMENTAL POR DESENHOS	BIOMETRIA FACIAL
COMPATIBILIDADE COM O MOODLE	SIM (FEITO PARA O MOODLE)	SIM (COM DIFICULDADES)	SIM (<i>WEB SERVICE</i>)
FORMA DE ATUAÇÃO	DETECTOR DE PLÁGIO	CONFIRMAÇÃO DE IDENTIDADE	CONTROLE DE ACESSO
AQUISIÇÃO	GRATUITO	PAGO	PAGO
HARDWARE	SEM HARDWARE ADICIONAL	SEM HARDWARE ADICIONAL	REQUER HARDWARE ADICIONAL

Fonte: Elaborado pelo autor (2016)

¹ Disponível em: <http://vmonaco.com/moodle-bioauth-plugin/>

² Disponível em: <https://www.biosig-id.com/industry/biosig-id-and-the-education-industry>

³ Disponível em: <https://www.entry.com.br/software/biometria-facial/faceid-biometria-facial/>

Essas ferramentas trabalham de formas diversas, e atuam na Segurança da Informação dos Sistemas de Informação a que se integram.

Monaco (2013), explica que a ferramenta BioAuth examina o padrão comportamental no momento da digitação do usuário do sistema. O BioAuth atua de forma integrada ao MOODLE, e pode ser estendido para a detecção de plágio. É gratuito para utilização, mas não para alteração do seu código. Além disso, a ferramenta não requer *hardware* adicional para seu uso.

Por outro lado, não encontramos estudos da eficácia dessa ferramenta, visto que algumas atividades são enviadas em forma de arquivo de texto, e esses arquivos podem ser feitos fora do AVA. Em outro aspecto, não foi encontrado informações sobre como essa ferramenta aborda o procedimento “copiar e colar”, que é um procedimento que pode ser utilizado pelos estudantes.

Segundo informações obtidas no site da ferramenta BioSig-ID, esta trabalha com biometria comportamental, onde o usuário fornece padrões de desenhos e combinações que posteriormente são calculadas biometricamente e comparadas com a base de dados. A ferramenta é disponibilizada através da contratação dos serviços. No uso da ferramenta, o usuário é autenticado através do seu comportamento ao desenhar as letras cadastradas. Trata-se de um método intrusivo e cansativo, que necessita de um treinamento complexo para identificar o usuário.

Além disso, o método pode ser influenciado pelo *hardware* do usuário, pois o *software* requer que os desenhos sejam feitos através dos periféricos de entrada, podendo sofrer alterações dependendo do dispositivo: marca, modelo, etc.

No site Entry da ferramenta Faceld, lê-se que a solução é disponibilizada com a contratação dos serviços e que pode ser utilizada por qualquer setor que busque uma autenticação através da biometria facial. A ferramenta trabalha com a utilização de serviços *web*, e redireciona o usuário para o sistema desejado. O sistema pode ser utilizado em AVAs se esse permitir acesso a serviços *web*.

O Faceld possui uma particularidade que dificulta a sua utilização na Educação a Distância: a ferramenta necessita de fotos com alta resolução para cadastro dos usuários, o que impossibilita o cadastramento de usuários que possuem computadores com câmeras de qualidade diferente das exigidas. Portanto, o sistema requer em muitos casos a compra de uma câmera de alta qualidade, apesar de ser um sistema robusto.

Na busca por soluções similares à do nosso estudo, a ferramenta RedFace foi encontrada. Porém ela não está disponível para *download*, sendo uma ferramenta de testes dos algoritmos de reconhecimento facial, e fruto de pesquisas acadêmicas para propor alternativas de autenticação em AVAS. Segundo Diniz et al (2013b, p. 2):

O RedFace adiciona a funcionalidade de autenticação biométrica ao AVA. Monitora um estudante, capturando imagens através de webcam, bem como detecta a face do estudante na imagem e a identifica dentre outras faces cadastradas no sistema.

O andamento da implementação da ferramenta RedFace para a autenticação em AVAs é desconhecido, porém Diniz (2013a) utilizou a ferramenta RedFace em seu trabalho de dissertação apresentado à Universidade Federal Rural do Semi-Árido. Em seu trabalho, o RedFace implementa o reconhecimento facial para reconhecer e classificar as emoções dos usuários dos AVAs. Portanto, não tem como objetivo a segurança da informação ou o monitoramento dos alunos.

Uma outra solução implementada em uma pesquisa de mestrado na Universidade Federal da Paraíba foi identificada no decorrer da pesquisa. A solução que recebeu o nome SIAF – EAD, usou a linguagem C++, e a biblioteca OPENCV (descrita no capítulo 3 deste trabalho) para criar um protótipo de identificação de usuários com arquitetura cliente-servidor (ROLIM, 2009). Porém o cadastro do usuário e a captura das imagens da face são realizadas de forma presencial, diretamente no servidor da aplicação. Para efetuar o ingresso na plataforma, o usuário deve ter o módulo de acesso instalado na máquina cliente. Diferente da solução SIAF – EAD, a ferramenta (RECOFACE) apontada por esta pesquisa efetua o cadastro do usuário e o ingresso na plataforma via *web*, e assim, possibilita a compatibilidade com um maior número de AVAs.

O sistema SIAF-EAD concentra seu trabalho na identificação do usuário, em que o sistema diz quem é o usuário. O SIAF-EAD não é focado na autenticação, onde a autenticação implicaria na confirmação ou negação da identidade invocada por uma pessoa. O SIAF-EAD não fornece a conveniência ao usuário de fazer seu cadastro sem se deslocar ao local do servidor. Além do exposto, no cadastro da face do usuário é preciso a presença de um especialista para selecionar as imagens da face para serem utilizadas no treinamento da aplicação.

Portanto, o sistema SIAF-EAD tem a preocupação com o monitoramento estudantil, através da identificação do estudante, não demonstrando uma preocupação com a segurança da informação nos AVAs.

O autor define seu sistema como:

[...] Sistema de Identificação Automática de Faces (SIAF-EAD) que adiciona ao MIF a funcionalidade de identificar por computador a real identidade de um usuário dentre outros usuários cadastrados. O SIAF-EAD é um sistema baseado na web composto de vários módulos que implementam o reconhecimento de faces utilizando a seleção de coeficientes da Transformada Discreta do Cosseno. Pretende-se que, com a utilização do SIAF-EAD, administradores, coordenadores, professores e tutores tenham uma certificação da participação de um aluno durante a realização de suas atividades e avaliações em um AVA. (ROLIM, 2009, p. 26).

Na continuação da pesquisa, foram identificados outros trabalhos que propunham modelos de arquitetura de *software* para autenticação em Ambientes Virtuais de Aprendizagem, porém sem a implementação de uma ferramenta específica, servindo apenas como modelos conceituais para serem utilizados na construção de *softwares* que realizam autenticação em AVAs através da biometria facial, ou não. Esses trabalhos são:

- Uma proposta de autenticação de usuários para Ensino a Distância (FIORESE, 2000).
- Autenticação biométrica de usuários em sistemas de *E-Learning* baseada em reconhecimento de faces a partir de vídeo (PENTEADO, 2009).
- Proposta de um modelo de autenticação segura para acesso a sites de ensino à distância utilizando biometria e cartões inteligentes (BERNARDI, 2007).

2.4.2 Comentários

Com a identificação de trabalhos e ferramentas similares a essa pesquisa, foi possível observar que a ferramenta gerada pelo presente estudo possibilita a integração de forma gratuita nos AVA da Educação a Distância, com a possibilidade

da manipulação da sua codificação para adequar-se ao AVA utilizado pela Instituição de Ensino.

O protótipo dessa pesquisa foi desenvolvido para ser executado via *web*, através de um navegador de internet. O cadastro das imagens da face e o cadastro do usuário no sistema é feito totalmente *on-line*. Com isso, possibilita aos professores, tutores, ou a qualquer membro envolvido com os AVAs da instituição, utilizarem a ferramenta no momento que desejar, fornecendo o endereço de acesso, registrando no banco de dados a validação das credenciais do aluno.

Além do exposto, o protótipo gerado por essa pesquisa pode ser acoplado ao AVA, inserindo as informações diretamente ao banco de dados da plataforma virtual. Isso é possível porque o protótipo foi desenvolvido com uma linguagem de programação muito utilizada no desenvolvimento de sistemas *web*. Portanto, a ferramenta realiza a autenticação do usuário, preocupando-se com a segurança da informação das plataformas de ensino, possibilitando a verificação da presença do estudante nos momentos determinados.

3 METODOLOGIA

No intuito de elaborar a ordem dos eventos de forma organizada no decorrer da pesquisa, obedecemos aos aspectos metodológicos expostos neste capítulo, que serve como orientação do trabalho e identifica como foi realizada a pesquisa, sua natureza, tipo, análise bibliográfica, métodos de coleta e análise dos dados, área de estudo e métodos utilizados no desenvolvimento.

A metodologia é um caminho a ser percorrido de forma lógica e pensamento ordenado (VERGARA, 2009). O presente estudo foi composto de três etapas. Na primeira etapa foi realizada uma pesquisa bibliográfica. Na segunda etapa foi realizada a elaboração e aplicação de um questionário para investigar a percepção dos integrantes da EAD do Instituto Federal do Piauí e da Universidade Federal do Piauí, acerca do uso da autenticação biométrica facial em Ambientes Virtuais de Aprendizagem, assim como questões voltadas para a segurança da informação e acompanhamento dos alunos. Com base na pesquisa bibliográfica e na análise dos dados coletados através do questionário, foi possível entender o problema, chegando na última etapa da pesquisa, que foi o desenvolvimento do protótipo de reconhecimento facial.

3.1 Tipo e natureza da pesquisa

Em sua primeira etapa, o presente estudo possui a tipologia de pesquisa bibliográfica exploratória. De acordo com Beuren (2010), a pesquisa exploratória tem como objetivo a realização de um estudo que aumente a relação do pesquisador com o assunto pesquisado, com a finalidade de tornar o entendimento evidente sobre o que é pesquisado.

Segundo Gil (1999, apud Beuren, 2010), a pesquisa bibliográfica realiza o estudo de conteúdos científicos anteriormente publicados, e através da análise desse material podemos obter dados necessários para a realização de uma nova pesquisa.

Como natureza da pesquisa, a abordagem qualitativa é utilizada, sendo complementada com a quantificação de dados. De acordo com Richardson (1999, apud BEUREN, 2010), a pesquisa qualitativa é caracterizada por não utilizar de métodos estatísticos para atingir seus resultados, tendo como objetivo verificar o comportamento das pessoas e analisar o assunto abordado. Contudo, é possível

utilizar métodos quantitativos para explicar fenômenos qualitativos. Embora sejam diferentes, tais métodos complementam-se, e realizam uma contribuição no trabalho de pesquisa, com uma mistura de procedimentos de cunho racional e interativo, capaz de levar a compreensão dos fenômenos analisados (POPE; MAYS, 1995 apud NEVES, 1996).

Tais processos são relacionados para atender ao primeiro e ao segundo objetivo específico, buscando averiguar a problemática que levou a esta pesquisa, de forma a caracterizar as maneiras de ingresso (*login*) e como é tratada a segurança da informação dentro das atuais ferramentas, observando o que elas dispõem e se preocupam. Além disso, foi realizada a identificação de ferramentas que utilizam biometria, sendo realizada um levantamento de trabalhos similares que abordam o uso da biometria em Ambientes Virtuais de Aprendizagem.

3.1.1 Métodos de coleta e análise dos dados

Na pesquisa, foi realizada a aplicação de um questionário como método de estudo exploratório, sendo aplicado para sujeitos que possuem experiência na EAD, como: estudante, professor conteudista, professor pesquisador, tutor presencial, tutor a distância e coordenador. Os respondentes puderam optar por mais de uma das opções aqui descritas, relatando terem mais de um tipo de experiência na EAD. As questões foram as mesmas para todos os sujeitos. Para Gil (2010), o questionário tem a vantagem de apresentar baixo custo de aplicação.

Os questionários foram aplicados de forma eletrônica, e não apresentaram custos na sua aplicação, pois foram criados na ferramenta *Google Forms*⁴. Inicialmente, o questionário passou por testes para adequar-se ao objeto da pesquisa, tendo sido testado com 4 (quatro) servidores do Instituto Federal do Piauí – IFPI. A titulação acadêmica dos 4 (quatro) servidores participantes do questionário de teste eram: 2 (dois) Doutores, 1 (um) Mestre e 1(um) especialista, todos com experiência na EAD. Os mesmos prontamente contribuíram com sugestões de alterações e adequações ao questionário.

Após o teste, o questionário foi distribuído através de *e-mails*, redes sociais como *WhatsApp* e *Facebook*, tendo como sujeito da pesquisa os membros que atuam

⁴ Disponível em: <https://docs.google.com/forms/>

ou atuaram na EAD do Instituto Federal do Piauí – IFPI e da Universidade Federal do Piauí – UFPI. O questionário foi disponibilizado por um período aproximado de 2 semanas, sendo encerrado quando as respostas cessaram.

A quantificação dos dados foi feita através da própria ferramenta *Google Forms*, que disponibilizou gráficos com as respostas dos respondentes. Além dos gráficos, a ferramenta disponibiliza a opção de transferir os dados para um arquivo do tipo .csv, que possibilita a exportação dos dados para aplicativos como o Excel e o Calc. Com isso, pode-se criar tabelas dinâmicas, que é um mecanismo desses aplicativos para auxiliar na análise dos dados. As respostas abertas foram analisadas com a abordagem qualitativa. O capítulo 4 apresenta os resultados e a discussão dos dados coletados no questionário.

3.2 Descrição da Pesquisa

Com o uso dos resultados obtidos pela pesquisa bibliográfica para argumentar acerca de assuntos tecnológicos dentro dos AVAs e dos resultados obtidos no questionário, foi possível entender a problematização em torno dos objetivos específicos a serem alcançados, levando a disposição de uma solução que possa atuar na problemática abordada na pesquisa.

O paradigma de pesquisa qualitativo, que segundo Mascarenhas (2012) é a pesquisa que é feita quando se irá descrever com profundidade o estudo realizado, conduziu o procedimento metodológico do trabalho, voltando o estudo para a segurança da informação que faz parte das áreas da ciência da informação, comunicação e computação.

A pesquisa teve a missão de codificar um protótipo nas linguagens PHP e Python, de forma a possibilitar a integração desse protótipo aos Ambiente Virtuais de Aprendizagem. Isso deve-se ao fato dessas linguagens de programação serem bastante utilizadas na programação para *Web*. Com isso, foi possível desenvolver uma ferramenta que realiza o reconhecimento facial, redirecionando o aluno após o reconhecimento para o AVA. No término do processo, o resultado é armazenado em um banco de dados.

A linguagem PHP foi utilizada para desenvolver o processo de *login* na ferramenta, trabalhando com um banco de dados para cadastro e consulta de usuários. Após o usuário fazer o ingresso na aplicação *web*, um *script* de

reconhecimento na linguagem Python é executado pela aplicação PHP. Após a execução do *script*, o navegador que executa a aplicação exibe os resultados. Esses resultados são os valores da verificação biométrica da face no banco de imagens, e usadas para armazenamento e posterior verificação da presença do aluno nos Ambientes Virtuais de Aprendizagem. Portanto a pesquisa teve um caráter experimental no desenvolvimento desse *software*, sendo necessário constantemente a execução de testes e novas codificações, a fim de obter uma ferramenta que promova os resultados esperados.

3.3 Metodologia de Desenvolvimento do protótipo

A área de concentração do estudo foi focada no desenvolvimento de ferramentas tecnológicas, apoiada nos dados obtidos na pesquisa e sua relevância. O processo metodológico da pesquisa obedece uma abordagem tecnicista e bastante utilizada na ciência da computação de forma geral, explorando a criação de protótipos que possivelmente servirão como um molde inicial e esboço para futuras criações e implementações que podem surgir.

O desenvolvimento de *software* possuiu peculiaridades. Na pesquisa foi preciso entender sobre aquilo que se desejava desenvolver, analisando os resultados do questionário para fortalecer a importância da criação da ferramenta. Além do estudo da melhor abordagem lógica na pesquisa e no desenvolvimento do protótipo, foi preciso analisar a problemática da pesquisa, relacionando-a com os fatores sociais e econômicos intrínsecos na implementação do protótipo e na escolha das ferramentas, percorrendo através da pesquisa bibliográfica uma análise do funcionamento dos AVAs e dos métodos que utilizam para autenticação.

Esses cuidados foram observados no decorrer da pesquisa, e são devidamente abordados no trabalho. Presman (2002) destaca que a comunidade que desenvolve *software* busca continuamente soluções para facilitar e agilizar o desenvolvimento, assim como tornar menos oneroso esse processo, prezando a qualidade e a melhoria contínua.

Segundo ASEE (2000, apud TAVARES et al, 2008), a engenharia é aplicação de princípios matemáticos e científicos, experiência, julgamento e bom senso para trazer coisas que beneficiam as pessoas. Depois dessa avaliação realística do projeto, a aplicação de técnicas de *Engenharia de Software* na construção se torna

imprescindível para organizar as ideias, as etapas, e os processos, realizando os incrementos necessários.

- Planejar cada requisito implementado;
- Planejar o desenvolvimento dos próximos módulos;
- Ter controle sobre os impedimentos encontrados, de forma a resolve-los rapidamente.
- Responder rapidamente a mudanças no projeto;

Na implementação da ferramenta, algumas etapas do desenvolvimento foram:

- Elaborar um projeto de como a aplicação irá funcionar;
- Escolher linguagens de programação;
- Determinar as funcionalidades da aplicação;
- Escolher ferramentas auxiliares para a construção do *software*;
- Verificar a compatibilidade com os navegadores atuais.
- Desenvolver, Testar e Manter a aplicação para confirmar as suas

funcionalidades.

Uma fase de teste foi necessária para descobrir eventuais falhas no *software* e favorecer a correção desses erros.

Abaixo estão destacados os procedimentos metodológicos que serviram para nortear o trabalho:

1. Concepção, Levantamento e Análise de Requisitos do protótipo.
2. Construção de uma base de dados local.
3. Criação do protótipo de *software* de reconhecimento facial.
4. Testes do protótipo e reflexão dos impedimentos encontrados.
5. Testes de *software* para verificar se o protótipo atende aos requisitos propostos inicialmente.

Sommerville (2003) lista em seu livro técnicas de levantamento de requisitos. A pesquisa utilizou algumas dessas técnicas. As técnicas de levantamento de requisitos utilizadas no estudo foram:

- Levantamento orientado a pontos de vista;
- Prototipagem;
- Questionário;

Os requisitos obtidos através do levantamento orientado a pontos de vista e através do questionário foram conseguidos através da aplicação do questionário da pesquisa com os membros da Educação a Distância do Instituto Federal do Piauí e da Universidade Federal do Piauí, conforme foi explicado anteriormente. O questionário explorou a percepção dos membros de forma mista, onde diferentes pontos de vista foram observados no questionário. Com isso, obtivemos as respostas necessárias para justificar a criação do protótipo.

A técnica de prototipagem foi explorada a medida que o protótipo foi desenvolvido. Pressman (1995), em seu trabalho sobre Engenharia de *Software*, define a prototipação como um processo que possibilita o desenvolvedor a criar um modelo do *software* que será desenvolvido. Com isso, foi possível obter os requisitos funcionais, definido como os requisitos que indicam as funcionalidades do protótipo, que são:

- Cadastro do usuário no protótipo;
- Tela para *Login* no protótipo;
- Rotina para acessar a *webcam*;
- Rotina para a captura de 3 imagens para cadastro da face;
- Rotina para armazenamento das imagens capturadas;
- Tela para captura das imagens para reconhecimento da face;
- Rotina para reconhecer a face do usuário;
- Rotina para emitir as mensagens de reconhecimento ou incompatibilidade no reconhecimento;
- Rotina para gravar no banco de dados as informações do reconhecimento;
- Rotina de redirecionamento para o endereço do AVA.

3.3.1 Materiais e Métodos

O protótipo de *software* construído usa a biblioteca OPENCV, utilizando seus métodos para implementação da detecção e do reconhecimento facial a partir de uma imagem, utilizando as linguagens PHP e Python.

O PHP é utilizado como linguagem de desenvolvimento da interface e responsável pela interação com o usuário através de um navegador de internet. Com o PHP é possível realizar o cadastro do usuário, além de trabalhar com a manipulação

dos arquivos necessários para o funcionamento do protótipo, gravar informações no banco de dados e receber informações dos *scripts* em Python.

Com a linguagem Python foi possível a criação de um *script* para manipulação das imagens capturadas, de forma a realizar a detecção facial, o treinamento e reconhecimento facial das imagens dos usuários, emitindo informações para o código escrito na linguagem PHP.

Como a aplicação é executada em um navegador *web*, as linguagens HTML e JAVASCRIPT foram utilizadas para complementar a interação com o usuário. A captura das imagens é realizada com Javascript e armazenadas pelo PHP.

3.4 OPENCV, PHP E PYTHON NA BIOMETRIA FACIAL

3.4.1 OPENCV

O OPENCV (*Intel Open Source Computer Library*) é uma extensa biblioteca disponibilizada para uso gratuito na área de computação gráfica e processamento de imagens. Foi desenvolvida pela Intel em 2000 e possibilitou uma gama de estudos com a utilização da mesma. No OPENCV existem diversas funções para um variado número de aplicações que facilitam o reconhecimento de padrões e o trabalho com visão computacional.

O OPENCV é muito utilizado profissionalmente e buscado pelos desenvolvedores para estudos. Isso deve-se ao fato de ser uma ferramenta *Open Source* e conter uma vasta documentação de uso. Muitas aplicações comerciais utilizam essa ferramenta, devido à sua eficiência e variedade de funções. O OPENCV é a biblioteca *Open Source* mais completa no campo da visão computacional (ZELINSKY, 2009).

Para ter acesso ao OPENCV, devemos fazer o *download* no site da ferramenta⁵. No site do OPENCV, devemos escolher a versão a ser baixada, e o Sistema Operacional que é utilizado pela máquina que recebe a instalação. É recomendado baixar a versão mais estável e mais atual, pois já passou por testes e correções de erros, além de ter funções atualizadas. Após executar o arquivo baixado, devemos escolher o diretório a ser instalado. Esse diretório é importante pois será utilizado como endereçamento das funções.

⁵ <http://opencv.org/downloads.html>

3.4.1.1 Bibliotecas do OPENCV

O OPENCV possui uma coleção de poderosas ferramentas destinadas ao desenvolvimento de aplicativos na área da visão computacional, como explicado anteriormente. Por ser uma ferramenta de livre utilização acadêmica e comercial, e por disponibilizar mecanismos para diagnosticar imagens em tempo real, a ferramenta tem sido bastante explorada. Desenvolvida originalmente na linguagem de programação C/C++, é possível utilizá-la em diversas plataformas de Sistema Operacional, explorando a compatibilidade da sua codificação.

O OPENCV tem sua biblioteca composta de funções para processamento de imagens e vídeos, estrutura de dados, entrada e saída de dados, interface gráfica básica do usuário com sistema independente de janelas, álgebra linear, controle de periféricos, além de centenas de algoritmos (GUIMARÃES, 2015).

Os principais módulos da biblioteca OPENCV segundo Guimarães (2015), são:

- cv: Contempla as funcionalidades e algoritmos destinados a visão computacional;
- cvaux: contempla os algoritmos destinados a área de visão computacional que ainda estão em fase experimental;
- cxcore: módulo de estruturas de dados e álgebra linear;
- highgui: módulo de controle de interface e dispositivos de entrada;
- ml: módulo de *Machine Learning*. Trata-se de um conjunto de classes e funções para a classificação estatística, *clustering*, etc;
- cvcam: módulo portátil para processamento de vídeo digital de câmeras;
- ed: trata-se de um manual de estrutura de dados e operações.

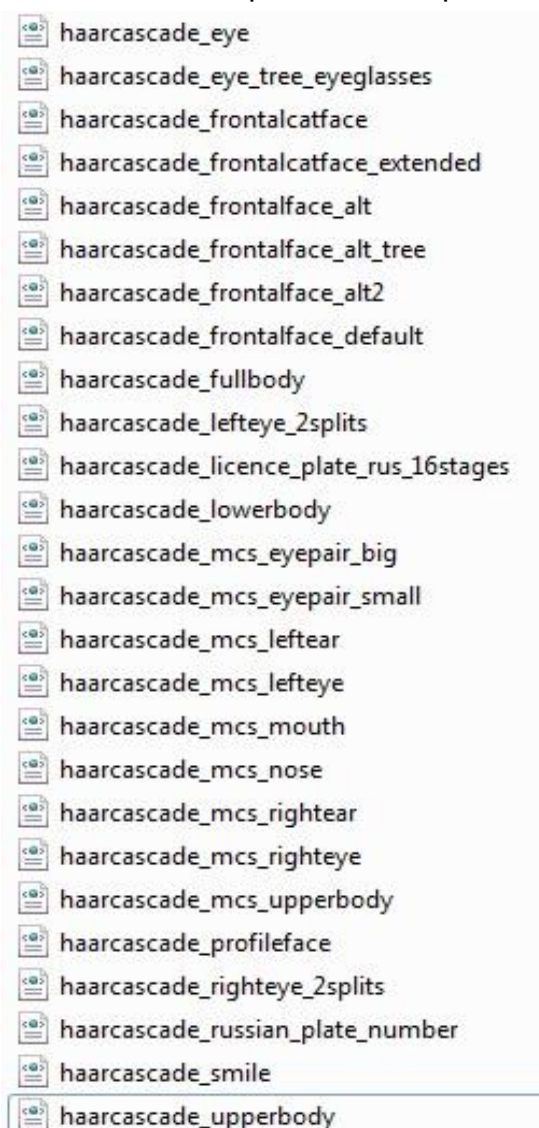
Na pesquisa, houve o estudo das ferramentas presentes na biblioteca OPENCV que auxiliam no processamento da imagem e na extração das características para o reconhecimento facial. O processamento da imagem tem a finalidade de melhorar o processo de reconhecimento facial, auxiliando os algoritmos de extração de características faciais. (GUIMARÃES, 2015).

Os algoritmos para reconhecimento facial na biblioteca OPENCV disponíveis atualmente são: O Eigenfaces, Fisherfaces, e Padrões binários locais de histogramas (LBPH) (OPENCV, 2016b). Para detecção facial, utilizamos o algoritmo *Haarcascade* que realiza a detecção frontal da face.

3.4.1.2 *Haarcascade*

O *HAARCASCADE* foi o método escolhido para realizar a detecção facial, visto a viabilidade de sua implementação utilizando a linguagem Python e a biblioteca *OPENCV*. O recurso *HAARCASCADE* é um classificador para detecção de padrões visuais de objetos. Aborda aprendizado de máquina, através do treinamento do código por um conjunto de imagens para então extrair características (OKABE, 2015). O *OPENCV* contém esses classificadores pré-qualificados para detecção de diversos padrões visuais (OKABE, 2015). Esses classificadores estão armazenados em arquivos XML (*Extensible Markup Language*), na pasta com endereço: `opencv/data/haarcascade`, disponibilizado após a instalação, conforme mostra a figura 4.

Figura 4: Classificadores disponibilizados pela ferramenta *OPENCV*



Fonte: Elaborado pelo autor (2016)

O arquivo XML utilizado no projeto para detecção de face é o `haarcascade_frontalface_alt.xml`.

Esse arquivo contém as características do rosto, utilizando o algoritmo implementado no OPENCV para detectar a face. As imagens são então reveladas quadro a quadro e ocorre a detecção da(s) face(s), onde são extraídas as características usando o algoritmo Viola-Jones, disponível na biblioteca OPENCV (OPENCV, 2016a).

O algoritmo Viola e Jones está implementado na biblioteca OPENCV, este algoritmo localiza características dos padrões buscados dentro de uma imagem (VIOLA; JONES, 2004). Esses padrões baseiam-se nas características de *Haar* que levam informações codificadas sobre os contrastes de uma imagem e suas regiões (BRADSKI; PISAREVSKY, 2000 apud GUIMARÃES, 2015). O algoritmo Viola e Jones é considerado um dos mais eficazes para detectar faces em imagens na forma estática (VIOLA; JONES, 2001; VIOLA; JONES, 2004). Portanto,

Este algoritmo tenta encontrar, em uma imagem, características que codificam alguma informação da classe a ser detectada. Para tal tarefa, são usadas as chamadas características de *Haar*, responsáveis por codificar informações sobre a existência de contrastes orientados entre regiões da imagem (DINIZ et al, 2012, p.4).

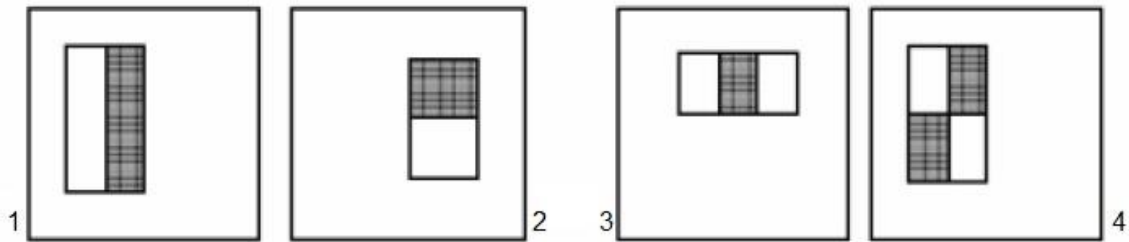
Viola e Jones (2001 apud MORAES, 2010) apresenta as características de *Haar* com a utilização de três formatos: Características de dois retângulos, características de três retângulos e características de quatro retângulos.

Característica de dois retângulos: Valor determinado pela diferença entre a soma dos pixels de duas regiões retangulares e vizinhas do mesmo tamanho.

Característica de três retângulos: Soma dos pixels de um retângulo central menos a soma dos pixels de dois retângulos externos.

Característica de quatro retângulos: Diferença entre os valores relativos aos pares diagonais de retângulos. A figura 5 apresenta o exemplo dos formatos das características de *Haar*.

Figura 5: Exemplo dos formatos das características de *Haar*. 1 - Dois retângulos na vertical; 2 - Dois retângulos na horizontal; 3 - Três retângulos; 4 - Quatro retângulos.



Fonte: Adaptado de VIOLA; JONES (2004 apud MORAES, 2010)

Viola e Jones (2004 apud GUIMARÃES, 2015) expõe que a fim de calcular as características de Haar, para que seja eficiente, é preciso uma representação intermediária chamada de imagem integral. Essa imagem integral é retirada da imagem original.

Para que se gere de forma rápida a imagem integral usando a imagem original, usa-se recorrentemente a equação:

$$s(x, y) = s(x, y - 1) + i(x, y)$$

$$ii(x, y) = ii(x - 1, y) + s(x, y)$$

Em que:

- ii é a imagem integral.
- $s(x, y)$ é a soma cumulativa da linha.
- $s(x, -1) = 0$
- $ii(-1, y) = 0$

Quando calculado o valor da imagem integral, o valor de qualquer área retangular é possível ser encontrada com a utilização dos quatro pontos dos vértices da área desejada (VIOLA; JONES, 2001 apud MORAES, 2010).

A função *Haarcascade* da OPENCV disponibiliza formas de reconhecimento de padrões diversos. Essas codificações estão agrupadas nos arquivos XML, que fornecem as informações resultantes do aprendizado de máquina para a construção do reconhecimento dos padrões. Esses arquivos XML podem ser lidos por diversas linguagens de programação através das funções disponibilizadas nas referidas linguagens. Logo,

A função *haarcascade* é utilizada para o reconhecimento da face e das características do indivíduo, que são arquivos .xml com os padrões pré reconhecidos de uma face, tais como boca, nariz, olhos, dentre outras; e não há necessidade fazer um *haarcascade* para cada indivíduo, pois todos os seres humanos possuem os mesmos padrões, porém suas características são únicas. (GUIMARÃES, 2015, p. 80).

Nas seções 3.4.1.3, 3.4.1.4 e 3.4.1.5, é abordado de forma conceitual os mecanismos de reconhecimento facial disponíveis na biblioteca OpenCV. O item 3.4.1.5 descreve o mecanismo utilizado na pesquisa. Portanto, é apresentado com maior ênfase.

3.4.1.3 Eigenface

O método *Eigenface* baseia-se em linearmente projetar o espaço de imagens em um espaço de características com dimensões reduzidas obtido com o uso da Análise de Componentes Principais (PCA), também conhecido como método Karhunen-Loeve (KINUTA et al, 2006). Por sua vez, devido à alta dimensionalidade no tratamento de vetores, é utilizada a técnica de Análise de Componentes Principais (PCA - *Principal Component Analysis*) de forma a reduzir a quantidade de características de uma imagem. (DINIZ et al., 2013b).

O *Eigenfaces* realiza uma busca por um conjunto de características que independe das formas anatômicas do rosto, como: olhos, nariz, orelhas e boca. Com, isso utiliza toda a informação da representação facial para reconhecimento de padrões faciais. (KSHIRSAGAR et al., 2011). Logo,

As *Eigenfaces* buscam identificar um pequeno número de características que são relevantes para diferenciar uma face de outras faces. Essas características podem ser analisadas apenas com a variação dos valores assumidos pelos pixels, em um conjunto de imagens de faces (DINIZ, 2013a, p. 54).

O método considera o reconhecimento facial como um problema de reconhecimento em 2 (duas) dimensões, com imagens das faces projetadas em um “espaço de faces” melhorando a representação da variação entre a face em questão e as já conhecidas (ALBERGARIA; SANTOS; ALVIM JÚNIOR, 2013). São formados autovetores do conjunto de faces, definidos como *Eigenfaces* (ALBERGARIA; SANTOS; ALVIM JÚNIOR, 2013).

O reconhecimento dá-se através do conjunto de treinamento, onde é calculado as *Eigenfaces*. Se a imagem for identificada como uma face, ocorre a classificação pelos padrões de pesos, relatando se é uma face conhecida ou não (ALBERGARIA; SANTOS; ALVIM JÚNIOR, 2013). A figura 6 apresenta um exemplo de *Eigenface*.

Figura 6: Exemplo de *Eigenface*



Fonte: OPENCV (2016b)

3.4.1.4 Fisherface

A Análise de Componentes Principais (PCA), é a base da técnica *Eigenfaces* (OPENCV, 2016b). E o método *Fisherface* utiliza como base, a técnica de Análise Discriminante Linear (LDA) (OPENCV, 2016b).

Nesse contexto, “A análise discriminante Linear (*Linear Discriminant Analysis* ou LDA) é um método estatístico que visa reduzir a dimensionalidade do espaço enquanto preserva o máximo possível de informações discriminatórias.” (BRAGA, 2013, p. 37).

Segundo Braga (2013), o LDA não é sensível à variação de luminosidade, mas é sensível à variação da identidade facial das pessoas. Isso é devido ao LDA selecionar o subespaço que melhor representa a classe de uma face.

O *Fisherface* é um método utilizado na extração de características e redução da dimensionalidade nos reconhecimentos de padrões (OKABE; CARRO, 2015).

A funcionalidade do Fisherface é dependente dos dados de entrada (OPENCV,2016b). Se o treinamento for realizado apenas com imagens com boa iluminação e os experimentos de teste com má iluminação, o método se torna susceptível a erros (OPENCV,2016b). A figura 7 apresenta um exemplo de Fisherface.

Figura 7: Exemplo de Fisherface



Fonte: OPENCV (2016b)

3.4.1.5 Padrões binários locais de histogramas (LBPH)

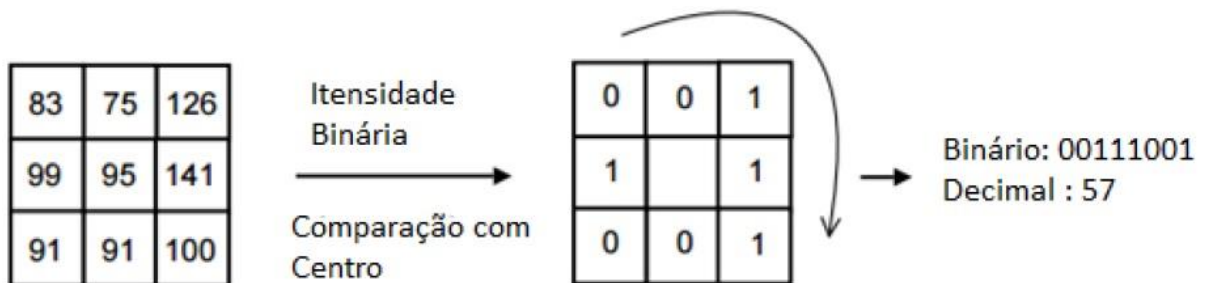
Os LBPs (*Local Binary Patterns*) foram inicialmente utilizados para a análise de texturas (OJALA; PIETIKAINEN; HARWOOD, 1996). Porém, é empregada em reconhecimento de faces com muito sucesso. Esta técnica faz com que uma imagem seja descrita como uma composição de micro padrões (SILVA, 2015).

Por isso, o seu grande sucesso na área de reconhecimento de identidade (AHONEN; HADID; PIETIKAINEN, 2006). Com isso,

O LBP tem como metodologia atribuir um valor binário para cada pixel da imagem. Este valor é determinado pela comparação de uma matriz quadrada contendo os pixels vizinhos, onde cada vizinho é comparado com o valor central. Isto ocorre quando se percorre cada pixel de uma imagem de modo a fazer uma análise levando em consideração a diferença entre os níveis de cinza deste pixel com os seus pixels vizinhos e, com isto, obtém-se o código local daquele pixel (SILVA, 2015, p.95).

O LBP quando utilizado em uma imagem, possibilita a concentração da estrutura espacial de parte da imagem (8 *pixels*) em um código LBP. O código é definido pela vizinhança de 3x3 *pixels*, e com a comparação dos *pixels* externos com o *pixel* central (NASCIMENTO, 2015). A figura 8 representa a operação para a obtenção do código LBP. Pode-se observar que a subtração dos pixels das bordas do pixel central for maior ou igual a 0, o valor 1 é atribuído. Caso seja menor que 0, o valor 0 é atribuído. O número binário 57 representa um micro padrão da estrutura.

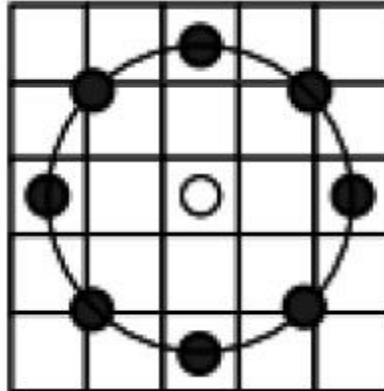
Figura 8: Demonstração da Operação LBP



Fonte: DEVI, S. S.; MANE, P. K.; AJAYKUMAR, D., (2012 apud NASCIMENTO, 2015)

O LBP foi estendido para calcular os códigos através do uso de círculos com diferentes raios, conforme é representado na figura 9. Com a utilização de interpolação, os pontos que não estão no centro são definidos (OJALA, T.; PIETIKAINEN, M.; MAENPAA, T., 2002 apud NASCIMENTO, 2015). Portanto, a face pode ser identificada com o uso de micro padrões com a utilização do LBP aliado ao uso de classificadores.

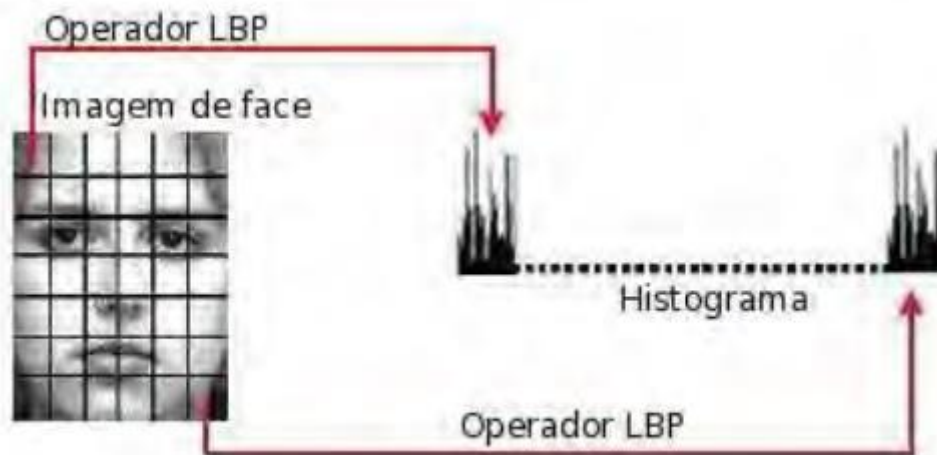
Figura 9: LBP Estendido



Fonte: DEVI, S. S.; MANE, P. K.; AJAYKUMAR, D., (2012 apud NASCIMENTO, 2015)

Quando calculado o LBP em cada *pixel* da imagem, por conseguinte são gerados os histogramas. Com a geração dos histogramas é formado o que é conhecido como descritor LBP, que é a distribuição de frequências dos valores dos operadores LBP utilizado para o reconhecimento facial (AHONEN; HADID; PIETIKÄINEN, 2006). Na figura 10 pode-se observar a ilustração da face com operadores LBP e o uso de histogramas.

Figura 10: Ilustração da face com operadores LBP e o uso de histogramas



Fonte: CHANG-YEON (2008 apud FARINA, 2012)

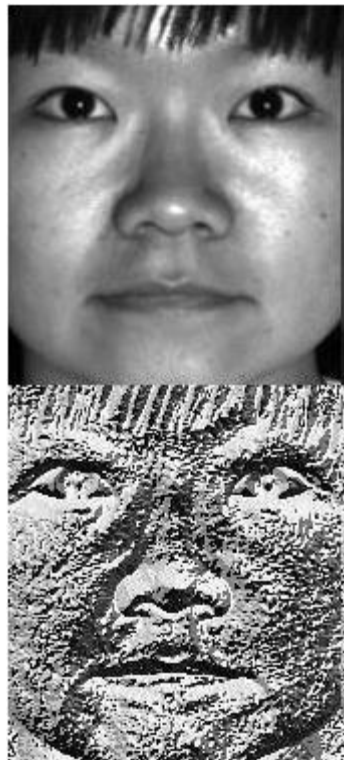
Eigenface e Fisherface abordam a questão de forma holística, onde os dados são tratados como um vetor em um espaço de alta dimensão (OPENCV, 2013b).

A abordagem Eigenface pode ter problemas se fontes externas gerarem uma variância na imagem (OPENCV,2013b). Da mesma forma, a abordagem Fisherface

pode ter problemas no reconhecimento, pois o método depende da imagem de entrada no momento do reconhecimento, devendo ser de forma mais idêntica possível com a imagem do treinamento (OPENCV,2013b). Desse modo, para o reconhecimento facial é utilizado o classificador de vizinho mais próximo aliado ao LBP e o uso de histogramas (LBPH) com raio de 1 e 8 vizinhos (AHONEN, T.; HADID, A.; PIETIKÄINEN, M., 2004).

Com base no exposto, o método LBPH da biblioteca OPENCV foi o método de escolha para ser aplicado na pesquisa e na criação do protótipo. Pois “ele provê um alto poder discriminativo e entre suas principais vantagens estão, sua invariância a luminosidade e eficiência computacional” (SILVA, 2014, p. 19). A motivação de utilizar o método para o reconhecimento facial, é devido ao fato de que faces podem ser vistas como uma composição de micro padrões que podem ser caracterizados por esse descritor (AHONEN; HADID; PIETIKAINEN, 2006). A figura 11 apresenta um exemplo de LBPH.

Figura 11: Exemplo de LPBH



Fonte: Adaptado de OPENCV (2016b)

3.4.2 PHP

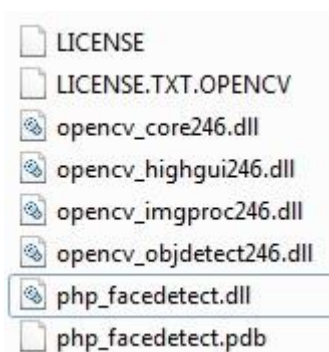
O PHP (Hypertext Preprocessor) é uma linguagem de programação utilizada em milhões de *sites* no mundo inteiro, sendo considerada uma das mais utilizada na *web* (NIEDERAUER, 2004). Uma das grandes vantagens do PHP é que ele é gratuito e de código aberto, e pode ser obtido no site da ferramenta⁶ (NIEDERAUER, 2004).

É necessário salientar que “o PHP vem adicionando mais e mais recursos e se consolida ano após ano como uma das linguagens de programação orientadas a objetos que mais crescem no mundo.” (DALL’OGLIO, 2015, p. 22).

Durante a pesquisa não foi encontrado funções que permitissem o reconhecimento facial utilizando a linguagem PHP de forma direta.

Portanto, para criar aplicações utilizáveis para biometria facial em PHP, devemos associar a linguagem PHP e outras linguagens de programação. Na construção do protótipo utilizando a tecnologia OPENCV, foi encontrado uma função chamada *PHP-FACEDETECT*⁷ que disponibiliza em seu método a detecção dos componentes do rosto como: nariz, face, olhos e boca. Essa função utiliza as funcionalidades das bibliotecas do OPENCV, obtendo parâmetros faciais encontrados na imagem, com a utilização das funções do pacote *Haarcascade* da OPENCV. Na figura 12, temos os arquivos contidos dentro da biblioteca *FACEDETECT* do PHP.

Figura 12: Arquivos da função FACEDETECT do PHP



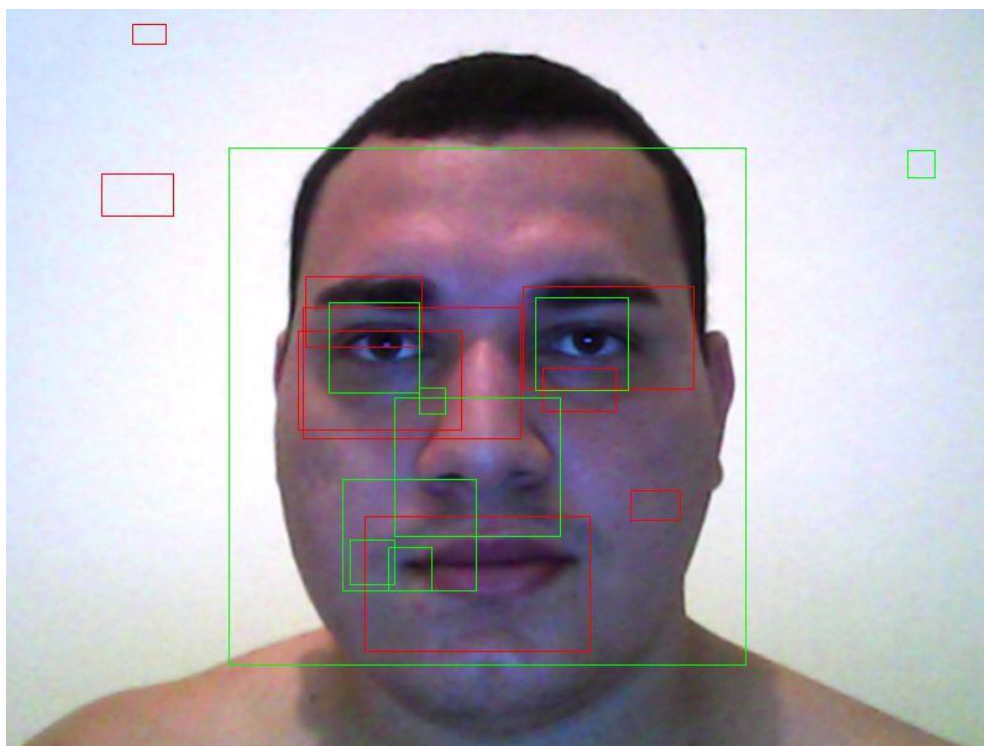
Fonte: Elaborado pelo autor (2016)

Com o uso do *Haarcascade*, e através da função *PHP-FACEDETECT* desenvolvidas para o PHP explorar a biblioteca *haarcascade* da OPENCV, foi possível obter um resultado preliminar como mostra a figura 13.

⁶ Disponível em: <http://www.php.net>

⁷ Disponível em: <https://github.com/infusion/PHP-Facedetect>

Figura 13: Resultado preliminar após executar o código feito em PHP para reconhecimento facial



Fonte: Elaborado pelo autor (2016)

O código realizado em PHP, utilizando a função *PHP-FACEDTECT*, explorou a biblioteca *haarcascade* de forma satisfatória, porém como a imagem não passou por nenhum tratamento e o código ainda ser primitivo, foi revelado falsos-positivos de detecção de padrões na imagem (Figura 13). O algoritmo foi elaborado para a realização de testes da eficácia do código.

O algoritmo de testes do *PHP-FACEDTECT* realiza uma pintura retangular sobre os padrões de olhos, nariz, boca e face encontrados. Houve uma distinção da cor do retângulo responsável por identificar os padrões bucais, pois são padrões mais fáceis de serem encontrados em um rosto, gerando uma gama de falsos-positivos.

Podemos observar que o resultado obtido na figura 13 não foi satisfatório, o código registrou diversos padrões erroneamente. O código deveria desenhar um retângulo em cada olho, no nariz, na boca e na face, porém os retângulos foram desenhados em outros espaços da imagem não correspondentes aos componentes faciais desejados.

Após os resultados obtidos, foi necessário um trabalho sobre a imagem para verificar se haveria alguma modificação no resultado. Como foi dito anteriormente, a imagem não passou por nenhum processamento, e somente com a redução do

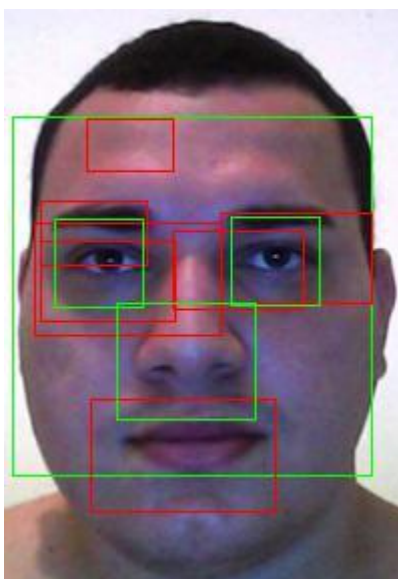
tamanho através de corte simples e redução da resolução da imagem, foi possível reduzir a quantidade de falsos-positivos encontrados na figura 13.

A figura 14, mostra os resultados obtidos após a edição simples (corte e redução da resolução) da imagem referenciada na figura 13. Em que foi evidenciado que para o recolhimento de parâmetros ser adequado, é necessário um trabalho de processamento de imagem.

Podemos observar na figura 14 que os falsos-positivos foram reduzidos aproximadamente em 57%, e que com a baixa da resolução da imagem, o algoritmo conseguiu identificar melhor o nariz, a boca, os olhos e a face.

Apesar do processamento da imagem realizado na figura 14 ser insuficiente, notou-se que a identificação dos componentes faciais foram mais confiáveis, porém a identificação dos padrões referente a boca, ainda continuaram a dar resultados inverídicos.

Figura 14: Resultado após a edição simples da imagem.



Fonte: Elaborado pelo autor (2016)

A função *PHP-FACEDETECT* realiza a detecção dos componentes da face, porém não trabalha com reconhecimento facial. Na pesquisa bibliográfica, realizada no trabalho, não foi encontrado funções do PHP que atuem de forma direta no reconhecimento facial utilizando PHP e OPENCV. Com isso, optou-se por utilizar no processo de detecção e reconhecimento facial a linguagem de programação Python, que é exposta na próxima seção.

3.4.3 PYTHON

O Python é uma linguagem de programação de código aberto, com sintaxe clara e concisa que favorece a legibilidade do código-fonte, tornando-a uma linguagem bem produtiva (BORGES, 2014). A linguagem inclui uma vasta coleção de módulos prontos para uso, além de ferramentas de terceiros que auxiliam no desenvolvimento, tendo a vantagem de ser portátil, onde o mesmo código pode executar em diversos Sistemas Operacionais (BORGES, 2014).

Para realizar o reconhecimento facial utilizando OPENCV e Python, é preciso a utilização de alguns módulos do Python, realizando a importação para o código escrito. Os módulos a serem importados dependem dos recursos que o desenvolvedor irá aplicar em sua ferramenta. Dentre os módulos necessários, podemos citar (HANZRA, 2015):

- cv2 - Este é o módulo que contém as funções de reconhecimento e detecção facial da OPENCV.
- os - Este módulo é utilizado para ter acesso a funcionalidades do Sistema Operacional utilizado. No reconhecimento facial pode ser utilizado para a extração de nomes de diretórios e de arquivos.
- Image - Este módulo fornece uma classe que é usada para representar uma imagem de PIL (Biblioteca do Python que realiza trabalhos com imagens). O módulo fornece várias funções que realizam carregamento de imagens, de arquivos e criação de novas imagens.
- numpy - É uma biblioteca otimizada para operações numéricas, trabalhando com matrizes.

Com a utilização de alguns módulos é possível implementar um *script* em Python para reconhecimento facial. Isso se deve a facilidade que o Python disponibiliza através da sua sintaxe concisa (HANZRA, 2015). Com isso, a linguagem Python possui os requisitos que foram necessários para a pesquisa e construção do protótipo, dando agilidade ao desenvolvimento, ao trabalho de treinamento e reconhecimento facial.

3.4.3.1 Hardware

O *hardware* utilizado na pesquisa foi:

- *Notebook* da fabricante ASUS com processador core i5 de 3ª geração e 6gb de memória RAM.
- *Webcam* ASUS USB 2.0.
- *Notebook* configurado com o Sistema Operacional Windows 8.1 Pro 64bits.

3.4.3.2 Software

Foi utilizado para o desenvolvimento do protótipo uma biblioteca de reconhecimento de padrões chamada OPENCV, que é totalmente livre para uso acadêmico e comercial, sendo desenvolvida pela Intel no ano de 2000, e destinada para o uso em aplicações de tempo real no campo da visão computacional.

Desenvolvida originalmente na linguagem de programação C/C++, ela é compatível para todas as plataformas de sistemas operacionais. Seu código fonte está disponível para que usuários possam alterá-lo, adequando-o a uma eventual necessidade particular. Possui módulos de processamento de imagens e vídeo, estrutura de dados, álgebra linear, interface gráfica do usuário (GUI), controle de mouse e teclado, além de mais de 2500 algoritmos, muitos dos quais são considerados estado da arte, tais como segmentação, detecção de faces (método Viola e Jones), aprendizado de máquinas, filtragem de imagens, rastreamento de movimento, entre outros métodos (OPENCV, 2001 apud DINIZ et al., 2013b).

Foi utilizado para desenvolvimento *web* o navegador Google Chrome versão 51.0 64bit e o aplicativo Wamp Server 2.4⁸, que possibilitou a criação de um servidor *web* local no computador utilizado. O Wamp Server é uma aplicação que contém várias tecnologias de forma conjunta, como o servidor Apache, o Sistemas Gerenciador de Banco de Dados MySQL e o servidor PHP para serem executados no Windows (TOLENTINO; TSUKAMOTO; NOMURA, 2013).

Além dos já citados, foi utilizado o interpretador da linguagem de programação Python 2.7⁹, e o editor de texto para auxílio na programação Sublime Text 3¹⁰.

⁸ Disponível em: <http://www.wampserver.com/en/>

⁹ Disponível em: <https://www.python.org/downloads/>

¹⁰ Disponível em: <https://www.sublimetext.com/>

3.4.3.3 Banco de dados

Foi utilizado o banco de dados Yale Face Database¹¹ que contém 165 imagens em tons de cinza de 15 indivíduos em formato gif. Há 11 imagens para cada indivíduo. Em cada imagem, o indivíduo tem uma expressão facial diferente, como feliz, triste, normal, surpreendido, sonolento, etc (HANZRA, 2015).

Utilizou-se um banco de dados com 10 imagens do total de 11 de cada indivíduo. O restante das imagens foram utilizadas para testar o algoritmo de reconhecimento de faces. Para cadastro e ingresso dos usuários na aplicação *Web* foi criado um banco de dados no gerenciador MySQL, que é acessado pelas rotinas executadas pelos códigos em PHP.

Além do banco de imagens Yale Face Database, foi criado um banco de imagens com o cadastro de 20 usuários no protótipo, onde cada usuário forneceu 4 imagens capturadas na *WebCam*, sendo 3 imagens para treinamento do algoritmo e 1 imagem para reconhecimento, totalizando 80 imagens. O cadastramento do usuário e a captura das imagens foi realizado com a linguagem PHP, e o processamento da imagem, detecção e reconhecimento da face foi realizado com a linguagem Python.

Para testes de desempenho foi criado um banco de imagens com 226 arquivos, onde o código foi executado realizando a comparação da imagem capturada para reconhecimento com o quantitativo total das imagens do banco (226 imagens), e executado comparando a imagem capturada para reconhecimento do aluno, apenas com as 3 imagens capturadas para cadastro e treino do algoritmo.

A figura 15 mostra um exemplo do conjunto de imagens de um sujeito do banco de imagens Yale Face Database e as variações de expressão para testar o algoritmo.

¹¹ Disponível em: <http://cvc.cs.yale.edu/cvc/projects/yalefaces/yalefaces.html>

Figura 15: Conjunto de imagens do Primeiro Indivíduo do Yale Face Database



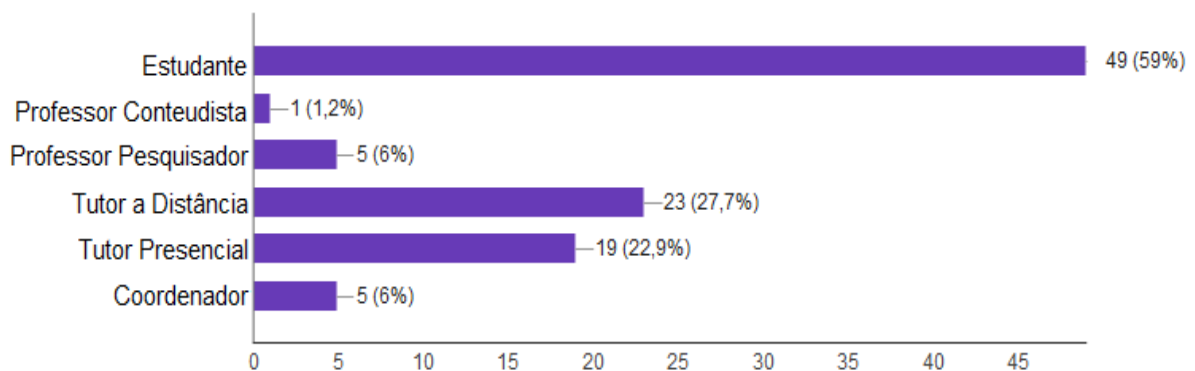
Fonte: XIANG (2006)

4 RESULTADOS E DISCUSSÃO PRELIMINAR

Este capítulo apresenta os resultados da pesquisa relativos aos dados obtidos na aplicação do questionário, realizando uma análise discursiva dos dados.

O questionário foi aplicado com pessoas que têm ou já tiveram envolvimento com a Educação a Distância na Universidade Federal do Piauí e no Instituto Federal do Piauí, desenvolvendo a sua experiência como estudante, professor, tutor ou coordenador. Participaram da pesquisa um total de 83 pessoas, entre estudantes, tutores presenciais, tutores a distância, coordenadores, professores conteudistas e professores pesquisadores. Os participantes que possuem experiência como estudantes da EAD registraram a maior frequência entre os participantes (59%), observando que na resposta ao questionário, o respondente poderia optar por mais de uma opção que tenha desempenhado na EAD, conforme mostra a Figura 16.

Figura 16: Atributos dos Respondentes na EAD

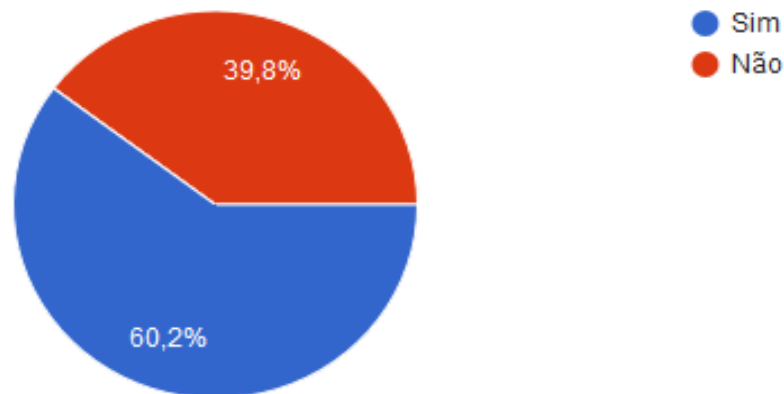


Fonte: Dados da pesquisa (2016)

Considerando o total de entrevistados, 60,2% responderam que consideram os AVAs propícios a fraude e 39,8% disseram que não (Figura 17).

Mesmo 39,8% dizendo que os AVA não são propícios a fraude (Figura 17), quando questionados sobre a importância do desenvolvimento de novas ferramentas tecnológicas, todos consideraram importante o desenvolvimento e o uso de novas ferramentas tecnológicas para melhoria da EAD, ou seja, 100% dos entrevistados.

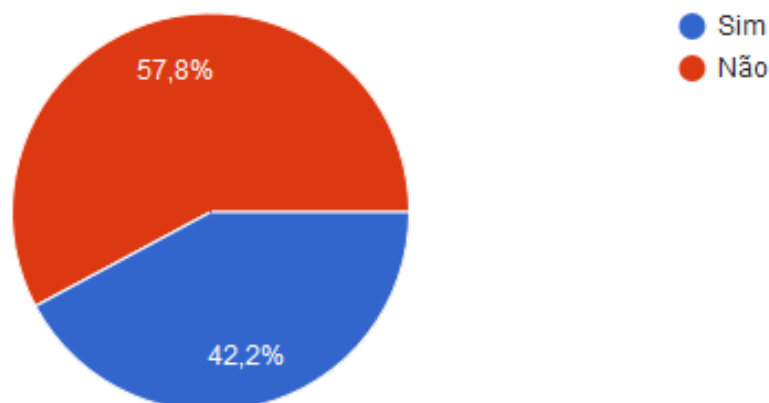
Figura 17: Opinião dos respondentes sobre a possibilidade de fraude em AVAs



Fonte: Dados da pesquisa (2016)

O método USUÁRIO/SENHA, mais utilizado na EAD para *login* (entrar) na plataforma de estudo, foi considerado por 57,8% dos entrevistados, insuficiente para garantir o monitoramento do aluno e também para garantir as horas de estudos, como pode ser observado na Figura 18.

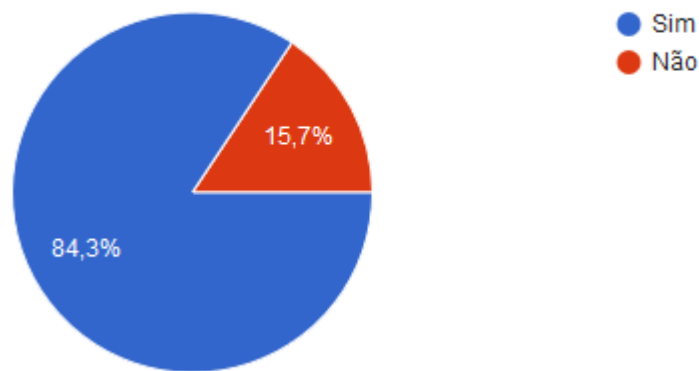
Figura 18: Respostas sobre a suficiência do método USUÁRIO/SENHA para ingresso nos AVAs



Fonte: Dados da Pesquisa (2016)

Como também, 42,2% disseram que sim, considerando esse método suficiente para garantir o acompanhamento dos alunos nos cursos da EAD. Porém, quando questionados sobre a utilização da biometria como forma de melhorar o monitoramento do estudante na EAD (Figura 19), 84,3% concordam que seria uma boa alternativa para melhorar o monitoramento dos estudantes.

Figura 19: Respostas sobre a biometria para melhorar o monitoramento do estudante na EAD

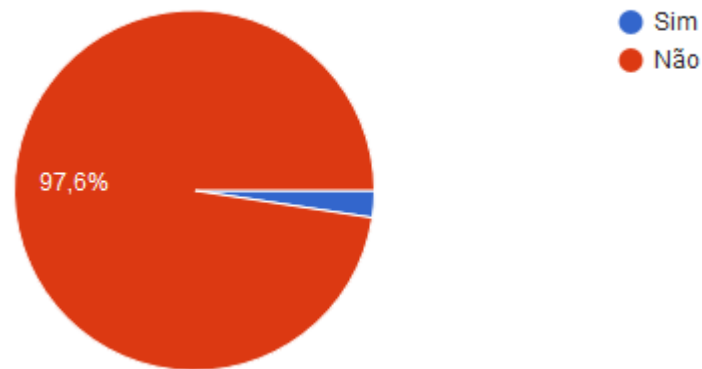


Fonte: Dados da Pesquisa (2016)

Somente 15,7% dos pesquisados responderam que a biometria não seria uma alternativa para o melhorar o monitoramento dos estudantes (Figura 19).

A falta de conhecimento por métodos biométricos de monitoramento dos estudantes em AVAs é de 97,6% (Figura 20), ou seja, métodos biométricos em AVAs são pouco conhecidos. Os 2,4% que relataram conhecer sistemas biométricos na educação, relataram que conhecem sistemas biométricos de frequência no ensino presencial, onde o aluno ao entrar na escola, registra-se biometricamente em um Sistema de Informação.

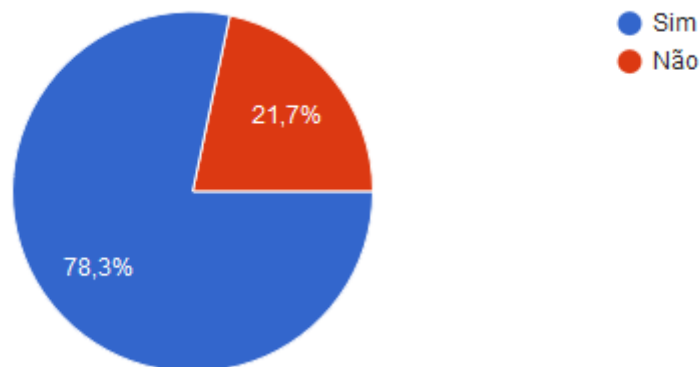
Figura 20: Respostas sobre outros métodos biométricos nos AVAs.



Fonte: Dados da Pesquisa (2016)

Em concordância com dados já obtidos, a figura 21 nos mostra que 78,3% dos respondentes concordam que a Biometria Facial como forma de *login* nas plataformas da EAD, melhoraria o monitoramento dos alunos. E apenas 21,7% não concordam que a biométrica seria uma alternativa para o melhorar o monitoramento dos alunos.

Figura 21: Respostas sobre a Biometria Facial na melhoria do monitoramento estudantil.



Fonte: Dados da Pesquisa (2016)

Quando perguntado o porquê, 63 pessoas responderam que isso melhoraria a segurança em ter o aluno presente, garantindo que ele é quem diz ser no momento do *login*.

Abaixo alguns dos comentários dos respondentes:

“Garante que a própria pessoa fez o login na plataforma, dessa maneira há garantia da presença do usuário e não qualquer pessoa que possua o login e a senha anotados em pedaço de papel, onde qualquer pessoa poderia acessar.”

“Garantiria que o aluno que está acessando os serviços disponibilizados através da web, realmente é quem ele afirma ser. Garantias de autenticidade.”

“Porque através da biometria facial o tutor saberá se é realmente o aluno quem estará usando o Ambiente Virtual de Aprendizagem e respondendo as atividades propostas.”

“A biometria evitaria a fraude no ensino a distância. Assim, teríamos a certeza que o aluno matriculado em determinado curso é o mesmo aluno que está participando ativamente das atividades solicitadas.”

“Porque evitaria que o aluno burle o acesso, somente com senha e usuário ele pode repassar a outra pessoa pra acessar. E com a biometria isso poderia ser evitado.”

“Por que inibiria de outro aluno logar na plataforma, a não ser com a presença do mesmo.”

“Dificultaria algum tipo de fraude que o estudante possa querer realizar.”

“Disponibilizaria novas técnicas de acompanhamento.”

“Como referência às aulas para se obter a Carteira Nacional de Habilitação. (Nesta não se tem o uso da EAD). Imagine o aluno para obter a CNH precisa da biometria que é feito presencialmente para comprovar o seu estudo. O aluno da EAD, com certeza é muito importante o uso da biometria. (Isso iria melhorar a qualidade e a segurança de todos nessa modalidade de ensino.).”

“Melhoraria, mas infelizmente não há suporte em todos os municípios, principalmente os de zona rural.”

Com a intenção de tornar os dados mais acessíveis ao entendimento, foi realizado uma filtragem através do uso de tabelas dinâmicas do aplicativo Excel, onde buscou-se obter informações sobre a quantidade de tutores a distância que tinham respondido, visto que os respondentes poderiam optar por mais de um tipo de experiência na Educação a Distância no momento que estava respondendo o questionário.

A tabela 1 discrimina os respondentes que relataram terem experiência como tutor a distância somente, ou somados a outra experiência.

Tabela 1: Respondentes com experiência como tutor a distância

Respondentes	Qual a sua experiência com a Educação a Distância (EAD)?
Estudante; Professor Pesquisador; Tutor a Distância	1
Estudante; Tutor a Distância	6
Professor Pesquisador; Tutor a Distância; Coordenador	1
Tutor a Distância	12
Tutor a Distância; Tutor Presencial	3
Total Geral	23

Fonte: Dados da Pesquisa (2016)

Quando realizado a filtragem das respostas dos tutores a distância sobre a possibilidade de fraudes nos AVAs, os resultados foram que 19 pessoas de 23, responderam que SIM (Tabela 2). Em valores percentuais, o resultado é que aproximadamente 82% responderam afirmativamente. Observando que 100% dos tutores a distância que já tiveram experiência como estudante, responderam que SIM.

Tabela 2: Opinião dos tutores a distância sobre possibilidade de fraudes nos AVAs

Você considera os Ambientes Virtuais de Aprendizagem (AVA) propícios a algum tipo de fraude?			
Experiência na EAD	NÃO	SIM	Total Geral
Estudante; Professor Pesquisador; Tutor a Distância	0	1	1
Estudante; Tutor a Distância	0	6	6
Professor Pesquisador; Tutor a Distância; Coordenador	0	1	1
Tutor a Distância	4	8	12
Tutor a Distância; Tutor Presencial	0	3	3
Total Geral	4	19	23

Fonte: Dados da Pesquisa (2016)

Quando questionados sobre a suficiência do método USUÁRIO/SENHA utilizado nos AVAs para garantir as horas de estudo dos alunos, aproximadamente 74% (17 respondentes) dos tutores a distância consideraram o método insuficiente. Esses dados estão sumarizados na Tabela 3. Observamos que 100% dos tutores a distância que já tiveram experiência como estudante responderam que NÃO.

Tabela 3: Suficiência do método Usuário/Senha segundo os Tutores a Distância

Se tratando da forma do estudante logar (entrar) na plataforma de estudo, você considera o método USUÁRIO/SENHA suficiente para garantir o monitoramento do aluno e garantir as horas de estudo?			
Experiência na EAD	Não	Sim	Total Geral
Estudante; Professor Pesquisador; Tutor a Distância	1	0	1
Estudante; Tutor a Distância	6	0	6
Professor Pesquisador; Tutor a Distância; Coordenador	1	0	1
Tutor a Distância	6	6	12
Tutor a Distância; Tutor Presencial	3	0	3
Total Geral	17	6	23

Fonte: Dados da Pesquisa (2016)

Em se tratando da biometria facial nos Ambientes Virtuais de Aprendizagem para melhorar o monitoramento do aluno na Educação a Distância, aproximadamente 82% dos tutores a distância (19 respondentes) escolheram a opção SIM, conforme vemos na tabela 4. Observamos que 5 dos 6 tutores a distância que possuem experiência como estudante disseram que a Biometria pode melhorar o monitoramento do aluno da EAD.

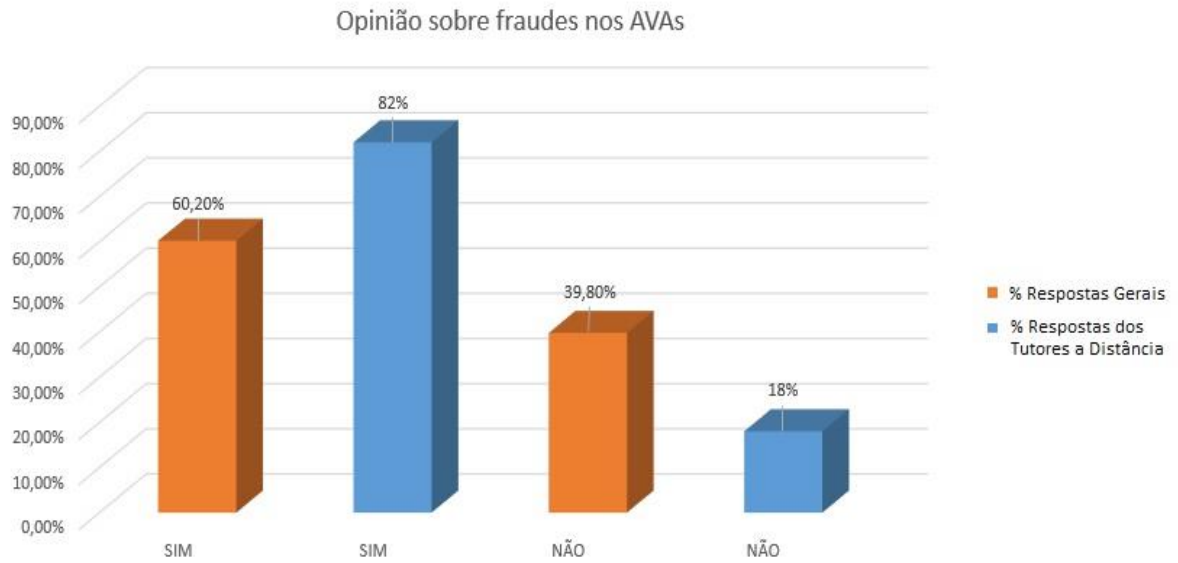
Tabela 4: Respostas dos tutores a distância sobre a viabilidade da biometria facial nos AVAs

A Biometria Facial como forma de logar nas plataformas melhoraria o monitoramento do aluno na EAD?				
Experiência na EAD	Não	Sim	Total Geral	
Estudante; Professor Pesquisador; Tutor a Distância	0	1	1	
Estudante; Tutor a Distância	1	5	6	
Professor Pesquisador; Tutor a Distância; Coordenador	0	1	1	
Tutor a Distância	2	10	12	
Tutor a Distância; Tutor Presencial	1	2	3	
Total Geral	4	19	23	

Fonte: Dados da Pesquisa (2016)

Quando comparados os percentuais das respostas gerais, com os percentuais das respostas dos tutores a distância em determinadas questões, houve uma variação significativa dos percentuais das perguntas 2 e 4 do questionário aplicado (Apêndice A). Conforme as figuras 22, 23 e 24. Na Figura 22, é mostrado o aumento do percentual da resposta “SIM” pelos tutores a distância na questão 2 do questionário, quando comparado com a porcentagem geral. A questão 2 aborda o tema sobre possibilidade de fraude na EAD.

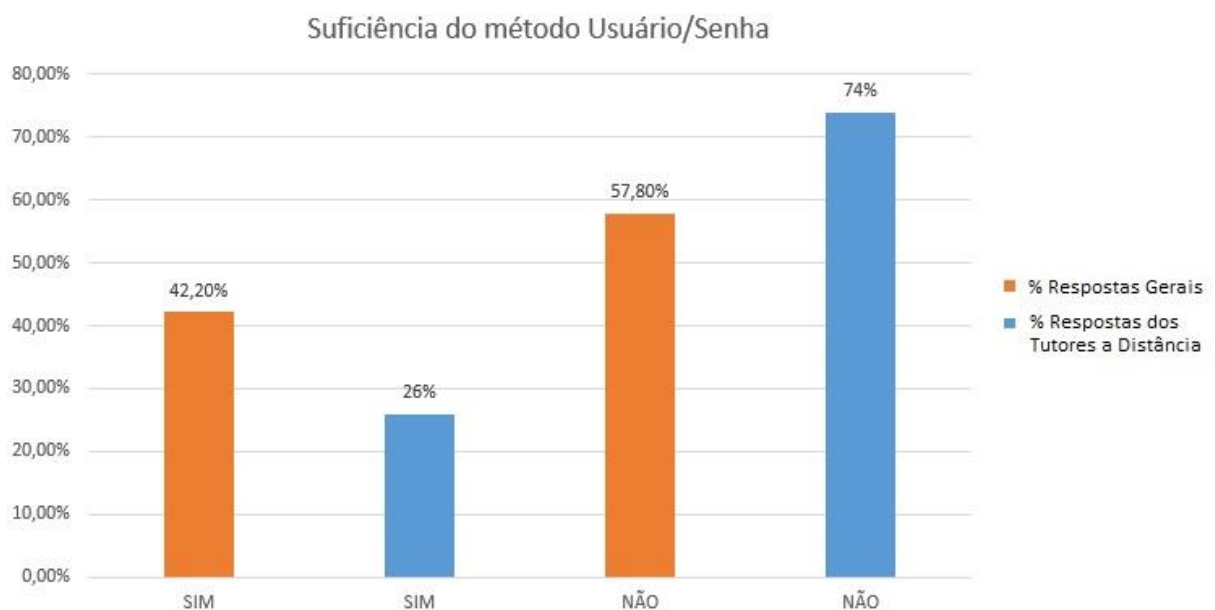
Figura 22: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 2.



Fonte: Dados da Pesquisa (2016)

Na Figura 23, é mostrado o aumento do percentual da resposta “NÃO” pelos tutores a distância na questão 4 do questionário, quando comparado com a porcentagem geral. A questão 4 aborda o tema sobre a suficiência do método Usuário/Senha nos AVAs.

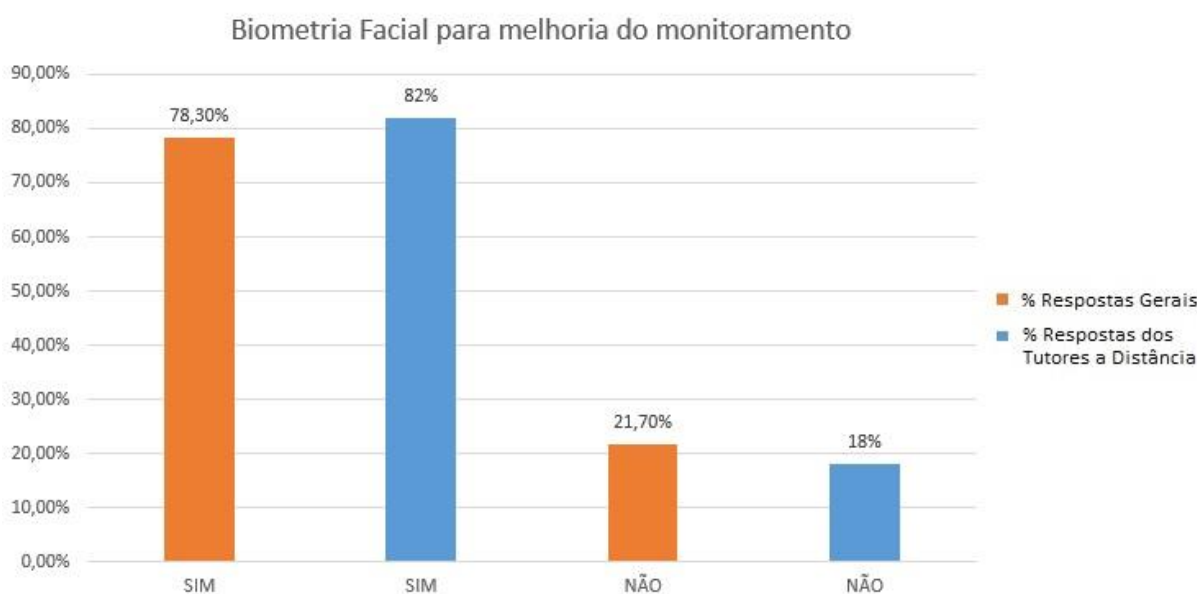
Figura 23: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 4.



Fonte: Dados da Pesquisa (2016)

Na Figura 24, é mostrado o aumento do percentual da resposta “SIM” pelos tutores a distância na questão 7 do questionário, quando comparado com a porcentagem geral. A questão 7 aborda o tema sobre a biometria facial na melhoria do monitoramento do aluno da EAD.

Figura 24: Comparação entre as respostas dos tutores a distância e as respostas gerais na questão 7.



Fonte: Dados da Pesquisa (2016)

4.1 Análise dos dados

A análise dos dados obtidos com o questionário indica que é relevante para a Educação a Distância a melhoria da segurança nos Ambientes Virtuais de Aprendizagem, sendo a biometria facial uma opção a ser considerada para essa melhoria. Com os dados coletados percebe-se que a maioria considerou os AVAs propícios a algum tipo de fraude, porém o questionário não explorou os possíveis tipos de fraude que os respondentes consideram ser possíveis.

Identificou-se que os respondentes, em sua maioria, consideram o método Usuário/Senha insuficiente para garantir o monitoramento das horas de estudo dos alunos da Educação a Distância. Quando questionados sobre a importância do desenvolvimento de novas ferramentas tecnológicas para a EAD, a resposta positiva

foi unânime. Com isso, a construção de pesquisas que abordem novas ferramentas tecnológicas para melhoria dos AVAs são justificadas.

Bernardi (2007); Fiorese (2000); Rabuzin; Baca e Sajko (2006); Rolim(2009); e Penteado (2009) abordam em suas pesquisas a importância da melhoria da segurança da informação nos Ambientes Virtuais de Aprendizagem com a implementação de mecanismos tecnológicos destinados a esse propósito. Rabuzin; Baca e Sajko (2006) relatam que o uso de mecanismos básicos para autenticação nos AVAs amplia a vulnerabilidade a fraudes. Fiorese (2000) discorre que a integração de múltiplos mecanismos de segurança da informação, reduz a possibilidade de fraudes.

Os sujeitos da pesquisa apontaram em sua maioria que mecanismos biométricos de forma geral influenciariam no monitoramento dos estudantes da EAD, aumentando a segurança da informação desses ambientes de aprendizagem. Quando perguntados sobre a biometria facial, que é o foco da pesquisa, os respondentes em sua grande maioria concordam que a biometria facial melhoraria a segurança da informação e o monitoramento dos alunos da EAD.

Corroborando com os resultados da pesquisa, Diniz et al (2013b) discorre sobre a importância dos mecanismos biométricos para a autenticação de alunos nos Ambientes Virtuais de Aprendizagem, e em seu trabalho propõe um mecanismo de autenticação por biometria facial para o monitoramento dos alunos e aumento da segurança da informação.

Assim como Diniz et al (2013b), Rolim (2009) propõe um mecanismo de reconhecimento facial para integração em Ambientes Virtuais de Aprendizagem, com o objetivo de monitorar os alunos, e aumentar a segurança da informação.

As pesquisas de Bernardi (2007); Fiorese (2000); e Penteado (2009) abordam de forma conceitual a implementação de ferramentas de biometria facial em Ambientes Virtuais de Aprendizagem, com a explanação da importância do método e a viabilidade de implementação. Os autores disponibilizam em sua pesquisa, arquiteturas de implementação do reconhecimento facial em plataformas virtuais.

Além disso, durante a pesquisa percebeu-se por parte dos sujeitos pesquisados que a grande maioria não conhece outros meios biométricos utilizados nos Ambientes Virtuais de Aprendizagem.

O aprofundamento do estudo voltado para os tutores a distância foi motivado pelo contato maior que o tutor a distância tem com os Ambientes Virtuais de Aprendizagem, e pelo seu contato com o estudante na maior parte do tempo ser

através dos ambientes virtuais, onde o tutor a distância realiza atividades, avaliações e registra a frequência desses alunos. Os tutores a distância que já foram estudantes da EAD trazem consigo uma experiência antagônica de sujeito avaliador e de sujeito avaliado, sendo a sua resposta relevante ao estudo.

A análise desta pesquisa sobre o uso da biometria facial nos Ambientes Virtuais de Aprendizagem mostrou que é desejável a utilização de meios biométricos nos Ambientes Virtuais de Aprendizagem, assim como evidenciou a biometria facial como uma opção viável como solução ao problema da pesquisa.

5 RESULTADOS E DISCUSSÃO DO PROTÓTIPO (RECOFACE)

Neste capítulo é abordado a descrição da ferramenta desenvolvida como solução para o problema da pesquisa, com a realização da descrição das tecnologias utilizadas, a descrição do protótipo, os testes realizados e resultados obtidos na implementação do protótipo.

5.1 Descrição do protótipo

O diferencial dessa ferramenta das demais formas de acesso biométrico, é a facilidade de encontrar os recursos de *hardware* para que funcione, onde o próprio Sistema Operacional pode fornecer o acesso aos dispositivos de captura de imagens. Certamente, os dispositivos de captura de imagens (câmeras digitais), são encontrados na grande maioria dos dispositivos modernos que são comercializados na atualidade. O uso da *webcam* tende a ser um dos pilares tecnológicos na EAD (PENTEADO; MARANA, 2009).

Para investigar a viabilidade de um sistema de controle baseado na biometria da face, foi desenvolvido um protótipo de tal sistema que atua na captura e reconhecimento da face, sendo capaz de detectar uma face em uma imagem estática e de efetuar o reconhecimento da face.

O protótipo é chamado de RECOFACE, e atua na captura de imagens para treinamento e imagens para reconhecimento. Para ter acesso às informações do protótipo, o usuário deve efetuar *login* através de um cadastro de usuário e senha, para posteriormente realizar a captura das imagens para treinamento e reconhecimento, como mostram as figuras 25, 26 e 27.

Figura 25: Cenário de funcionamento do RECOFACE



Fonte: Elaborado pelo autor (2016)

Figura 26: Tela Inicial do RECOFACE



Fonte: Elaborado pelo autor (2016)

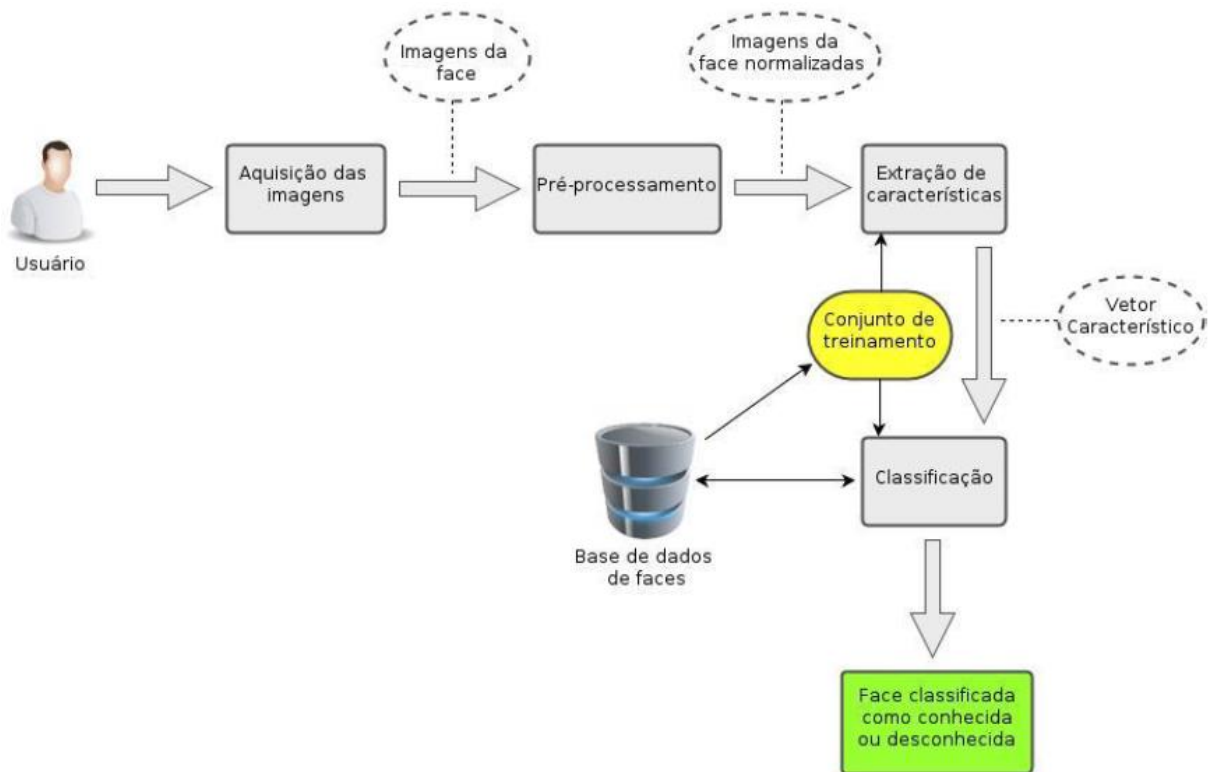
Figura 27: Tela Após efetuar o ingresso no RECOFACE



Fonte: Elaborado pelo autor (2016)

O RECOFACE trabalha com os algoritmos de detecção de faces e de reconhecimento de faces da biblioteca OPENCV, mais especificamente usando o `haarcascade_frontalface_default.xml` e os métodos da biblioteca `cv2` utilizados no *script* Python, como a função `cv2.createLBPHFaceRecognizer()`. As funções do `cv2` no *script* Python são utilizadas para converter a imagem em escalas de cinza, detecção da face, treinamento e reconhecimento da face cadastrada pelo usuário no protótipo RECOFACE. A figura 28 mostra a arquitetura do RECOFACE.

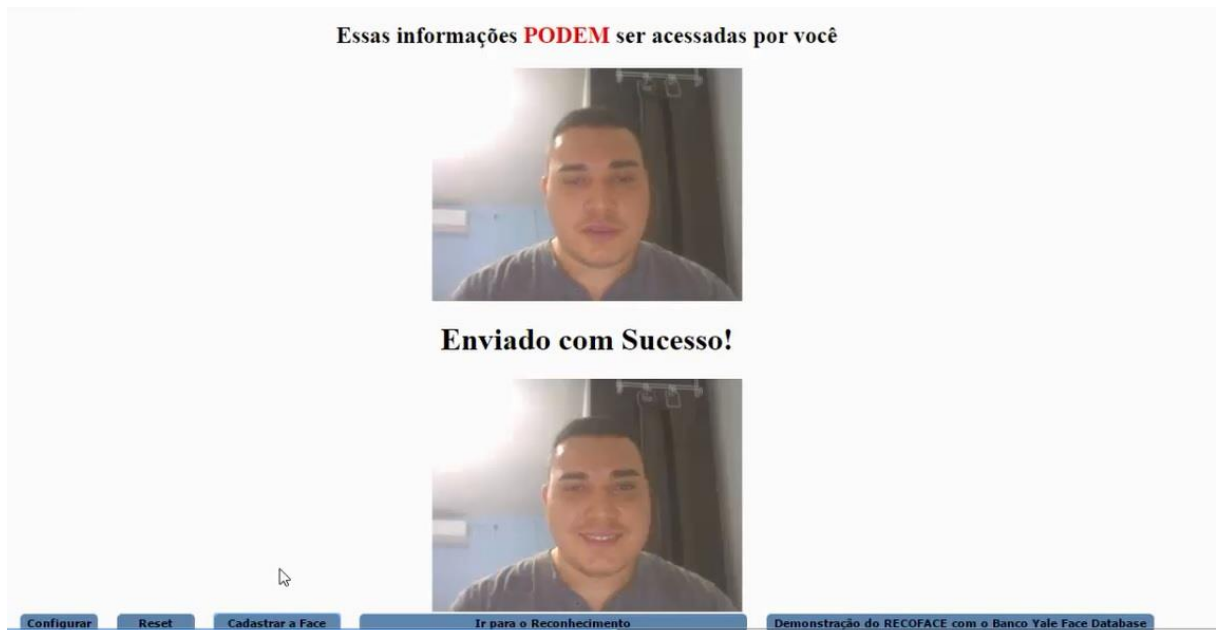
Figura 28: Arquitetura do protótipo



Fonte: (DINIZ et al., 2013b).

Partindo do pressuposto que os padrões faciais são características únicas ou no mínimo raras, após o ingresso no RECOFACE, o usuário deve fornecer 3 (três) imagens da sua face no momento do cadastro no protótipo. O RECOFACE realiza a captura das imagens em um tamanho fixo de 320x240 *pixels*, configurado de forma rígida na programação do protótipo no momento da captura das imagens pela *webcam*. Essas imagens compõem o banco de imagens de usuários do protótipo, servindo de base para o treinamento do algoritmo, e para criação do banco de imagens dos usuários cadastrados no RECOFACE, como mostra a figura 29.

Figura 29: Enviando para o servidor as imagens para treinamento



Fonte: Elaborado pelo autor (2016)

Após a realização do cadastro das imagens para treinamento, o RECOFACE possui uma página destinada para o reconhecimento do usuário. Nessa página o usuário realiza uma captura de sua face, e após o envio dessa imagem o usuário pode realizar o reconhecimento da sua face (Figura 30). Quando o usuário ativa o botão do reconhecimento, o RECOFACE processa a imagem e emite uma mensagem de reconhecimento da face ou face não reconhecida.

É emitido também uma taxa de confiança da imagem reconhecida, em comparação com as faces cadastradas para treinamento. Quando o usuário ativa o reconhecimento, suas informações de identificação de usuário, de data e hora da execução do reconhecimento, e a mensagem emitida, são armazenada no banco de dados da aplicação. Após a execução do reconhecimento, o usuário é redirecionado para o AVA.

Figura 30: Página de realização do Reconhecimento



Fonte: Elaborado pelo autor (2016)

Outra particularidade do método é que o estudante fornecerá o usuário e a sua senha para iniciar a sua sessão no protótipo. Após a sessão iniciada, os parâmetros faciais são requisitados para verificação da validade do *login*, atestando que o usuário é realmente quem diz ser. Essa rotina é importante para que o desempenho do programa seja amplificado, e para que o programa tenha as variáveis necessárias para a implementação da lógica de programação utilizada no RECOFACE.

5.2 Testes, Resultados e Análise

5.2.1 Testes do Protótipo

Na construção do algoritmo do protótipo foi realizado testes com bancos de imagens para atestar a funcionalidade do código e prosseguir com a implementação da solução proposta. O algoritmo de detecção e reconhecimento foi escrito na linguagem Python conforme exposto anteriormente, o que proporcionou agilidade no desenvolvimento.

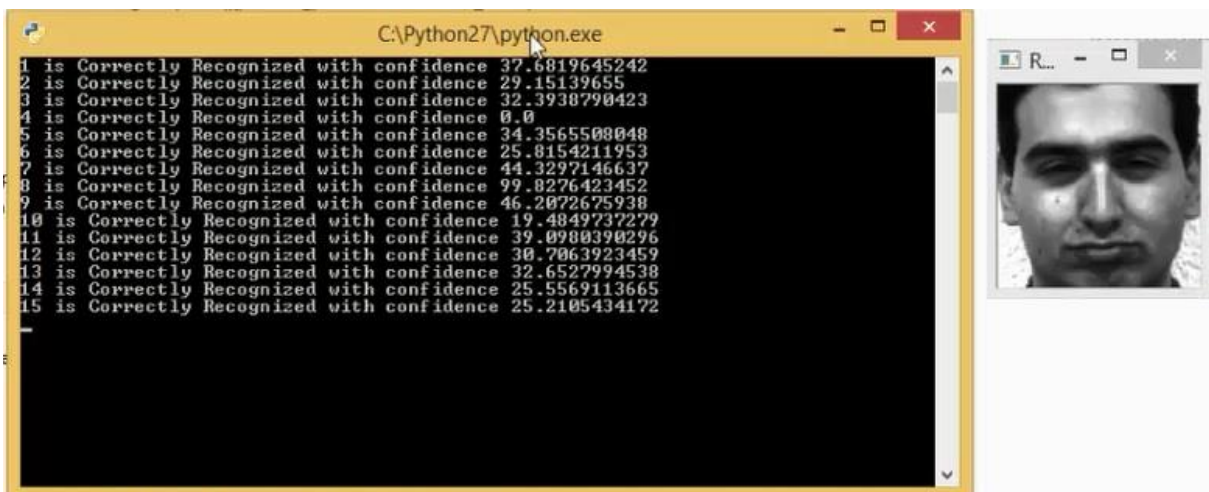
O código Python, em sua execução, pega o endereço de armazenamento das imagens para treinamento e o nome das imagens, com isso, realiza a criação de uma

matriz com essas informações. Na execução, cada tupla da matriz possui as faces encontradas nas imagens e um identificador gerado pelo nome da imagem gravada no disco local. As faces são detectadas com o uso do componente *haarcascade_frontalface_default.xml* da biblioteca OPENCV e passam por um processo de conversão da escala de cores da imagem, convertendo para a escala de cinzas. Essa conversão tem o objetivo de facilitar a detecção da face e o reconhecimento, equalizando os tons e contornos das formas da imagem.

Durante o treinamento, o algoritmo necessita ter o identificador da imagem e a própria imagem para extração das características, atribuindo o valor dessas características ao identificador. Após a realização do treinamento, o algoritmo recebe uma imagem distinta às imagens do treinamento, realizando uma comparação de características e emitindo uma mensagem de identificação positiva, ou de identificação negativa.

No teste de funcionalidade do algoritmo em Python, foi utilizado o banco de imagens Yale Face Database. A figura 31 mostra os resultados do teste do algoritmo.

Figura 31: Resultado do teste do algoritmo Python com o banco de imagens Yale Face Database



Fonte: Elaborado pelo autor (2016)

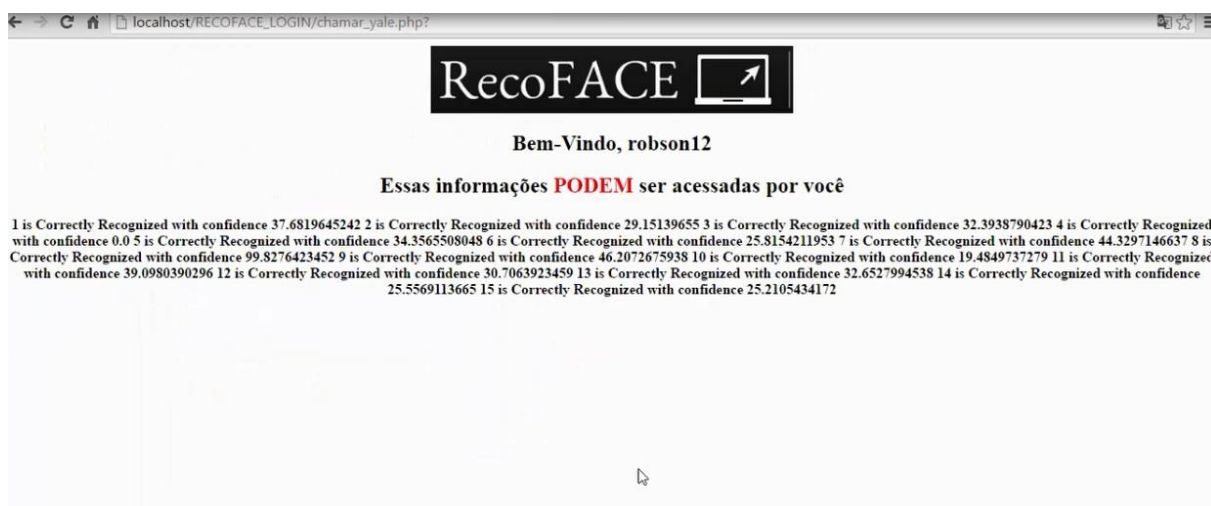
Após os testes do algoritmo em Python e os resultados obtidos, foi possível avançar para a codificação na linguagem PHP. Na codificação em PHP, foi gerado um código para realização de autenticação no momento de ingresso no sistema RECOFACE. Essa autenticação foi necessária, pois com ela é possível gerar variáveis para identificação do usuário, facilitando o armazenamento das imagens e a identificação do mesmo no momento do treinamento e do reconhecimento. Além de

facilitar o encadeamento lógico do código Python, possibilita ao sistema o incremento da segurança da informação trafegada.

Com a criação do sistema de autenticação por meio do usuário e senha no PHP, foi possível criar um ambiente seguro e com as variáveis necessárias para a implementação do restante do protótipo. Com isso, surgiu um novo desafio na implementação que foi fazer com que a codificação em PHP realizasse a execução do algoritmo Python e obtivesse o resultado do reconhecimento. Esse desafio foi superado com a utilização da linha de código PHP: `System("face_recognizer.py");`.

Com essa função foi possível executar um código Python na máquina local e obter o valor para o RECOFACE no navegador que o está executando. Conforme a figura 32, que mostra o resultado da execução do código Python, executado com o banco Yale Face Database.

Figura 32: Resultado do código Python chamado pelo código PHP do RECOFACE



Fonte: Elaborado pelo autor (2016)

Após a verificação da viabilidade do processo de construção do RECOFACE utilizando Python e PHP, foi possível arquitetar o funcionamento lógico do RECOFACE.

Com o *login* devidamente efetuado pelo usuário, o sistema requisita a captura de imagens para cadastro da face. Essas imagens capturadas no cadastro são destinadas ao treinamento do algoritmo, que no protótipo são em um número de 3 (três) por usuário. Em seguida, o usuário pode redirecionar-se para a interface de reconhecimento, onde realiza a captura da imagem para reconhecimento.

A princípio, na pasta raiz do RECOFACE foi criado duas pastas para armazenamento das fotos capturadas pelo protótipo. A pasta uploads e a pasta

reconhecimento. Na pasta uploads foi armazenado as imagens para treinamento do algoritmo, contendo as imagens realizadas no cadastro, e na pasta reconhecimento foi armazenado uma pasta para cada usuário que realizou a captura para o reconhecimento na interface de reconhecimento. A pasta reconhecimento possui arquivos necessário para a execução do reconhecimento do usuário com a foto capturada.

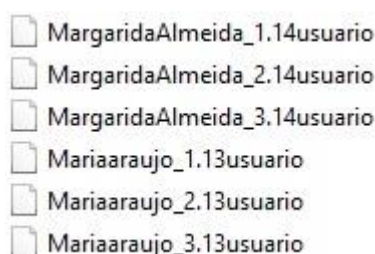
Após a construção do protótipo, foi realizado o cadastramento de 20 usuários para testes no RECOFACE. No decorrer dos testes, foi realizado a captura de imagens e reconhecimento dessas, para obter um nível de confiança do reconhecimento dos usuários autenticados no sistema. Ou seja, os 20 usuários que cadastraram-se no RECOFACE foram submetidos a testes de reconhecimento.

No prosseguimento dos testes, 5 usuários se autenticaram com usuário e senha de outro usuário cadastrado no RECOFACE, simulando um momento de fraude e tentando burlar o sistema de reconhecimento facial. Além dos testes relatados, foi montado um banco de imagens com 226 imagens para testar o desempenho do RECOFACE no momento do reconhecimento.

5.2.2 Resultados obtidos

Com a arquitetura elaborada para o funcionamento descrita anteriormente, foi possível nomear as imagens gravadas pelo RECOFACE da maneira adequada para a utilização das imagens pelo código Python. Como mostra a figura 33.

Figura 33: Exemplo de imagens salvas pelo RECOFACE com a nomeação adequada para o uso do código Python



Fonte: Elaborado pelo autor (2016)

O código PHP foi responsável por salvar e nomear as imagens capturas dos usuários, ordenando em pastas e salvando com nomes que possibilitem a correta

identificação e utilização pelo código Python. Com isso, o código Python obteve as variáveis necessárias para a execução e identificação do usuário autenticado no RECOFACE. Na figura 34 temos um exemplo de imagens capturadas para treinamento e identificação dos usuários no momento da execução do código Python.

Figura 34: Exemplo de imagens dos usuários capturadas pelo código em PHP e processada pelo código Python



Fonte: Elaborado pelo autor (2016)

O processamento da informação foi possibilitado com o ordenamento lógico das variáveis obtidas desde o momento do *login* do usuário, até o resultado do reconhecimento. Através dos recursos utilizados que foram descritos anteriormente, o protótipo RECOFACE conseguiu reconhecer as imagens dos usuários cadastrados, emitindo o resultado do reconhecimento e um nível de confiança em uma escala que vai de 0 a 100. Nessa escala, quanto mais próximo de 0 for o resultado, maior o índice de confiança. No resultado do reconhecimento, o RECOFACE emite o número de identificação do usuário, que é gerado no momento do cadastramento do *login* por usuário e senha.

A figura 35 mostra o resultado do reconhecimento do usuário de identificação 5, que obteve o nível de confiança de 34,9196399282. Caso o usuário não seja reconhecido, o sistema retorna a mensagem “Face incompatível”.

Figura 35: Resultado do reconhecimento do usuário de identificação 5.

COFACE_LOGIN/reconhecimento/robson12/chamar_python.php?



Bem-Vindo, robson12

Essas informações **PODEM ser acessadas por você**

Usuário de identificação-5, a face foi reconhecida com confiança de: 34.9196399282

Fonte: Elaborado pelo autor (2016)

No teste do algoritmo de reconhecimento na linguagem Python que foi executado com o banco de imagens Yale Face Database, todas as imagens destinadas ao reconhecimento foram identificadas corretamente com base nas imagens destinadas ao treinamento do algoritmo.

O cadastramento dos 20 usuários foi efetuado sem a ocorrência de problemas, tanto no cadastramento do usuário e da senha, quanto no cadastramento das imagens para treinamento. No reconhecimento dos usuários, o RECOFACE conseguiu identificar corretamente os usuários que entraram no sistema com seu usuário e senha verdadeiros, obtidos no momento do cadastro. O RECOFACE obteve êxito reconhecendo os usuários que seguiram as orientações no momento da captura das imagens para treinamento e para reconhecimento.

É importante ressaltar as limitações do trabalho no cadastramento dos 20 usuários. Além de ser uma base de dados pequena, o cadastramento foi realizado com condições limitadas. Não houve variações significativas de planos de fundo, iluminação, angulações da face ou de *hardware* utilizado. No momento do cadastro, os usuários foram orientados como proceder na captura das imagens, procedendo apenas com variações das expressões faciais.

Os 5 usuários que tentaram burlar o RECOFACE tiveram êxito quando burlaram o usuário e senha passados por terceiros, ou seja, utilizando as credenciais falsas. Porém quando tentaram o reconhecimento da face, o sistema recusou o usuário, retornando a mensagem “Face Incompatível.”

5.2.3 Análise dos Resultados

Os resultados obtidos no teste do algoritmo Python utilizando o banco de imagens Yale Face Database logrou êxito e deu ao trabalho a ferramenta necessária para o prosseguimento no andamento da codificação. Com isso, foi possível obter um código base para o reconhecimento de forma eficiente, dando continuidade na construção do protótipo.

Na construção do protótipo, a linguagem PHP se mostrou eficiente no trabalho com os arquivos e na criação de diretórios, possibilitando o encadeamento lógico necessário para a execução do código de reconhecimento em Python. Dos 20 usuários cadastrados no RECOFACE, todos foram reconhecidos pelo sistema. Os usuários seguiram as orientações dadas pelo sistema no momento do cadastro e no momento do reconhecimento, proporcionando uma melhor atuação do protótipo de reconhecimento facial que pode ser prejudicado quando as orientações não são seguidas.

Nos testes criados para simular uma tentativa de fraude ao sistema RECOFACE, as fraudes só foram possíveis na primeira etapa da autenticação, que corresponde à disponibilização das credenciais de usuários e senha. O usuário e senha se enquadram no quesito “aquilo que o usuário conhece”, que pode ser passado para um terceiro. No entanto, quando a autenticação é validada com o reconhecimento facial, os usuários não concluíram a tentativa de fraude simulada, pois o reconhecimento facial é a autenticação caracterizada por ser aquilo que o usuário é fisicamente.

No teste de desempenho do algoritmo, à medida que os cadastros foram efetuados, o desempenho do código de reconhecimento foi tornando-se lento em sua execução, diminuindo a agilidade do retorno das informações do RECOFACE. Isso ocorreu devido a quantidade de imagens que eram gravadas na pasta uploads, pasta destinada a armazenar as capturas feitas para o treinamento do algoritmo, visto que o código que realiza o treinamento e o reconhecimento das imagens são executados de uma única vez, no mesmo código Python.

No teste de desempenho foram depositadas um quantitativo de 226 imagens na pasta de uploads, e calculado o tempo de execução do reconhecimento que foi de aproximadamente 15 segundos para obter o resultado. Foi observado que quando o banco de imagens estivesse com um quantitativo elevado de imagens, o sistema teria

seu desempenho comprometido, necessitando uma mudança na arquitetura dos arquivos de treinamento do protótipo. Com isso, uma nova estratégia de armazenamento foi criada para que as imagens de treinamento fossem gravadas individualmente por usuário. Ou seja, cada usuário teve suas fotos de treinamento separadas das fotos dos demais usuários em pastas destinadas para cada usuário dentro do sistema. Com a alteração, o tempo de resposta do código de reconhecimento foi reduzido para aproximadamente 1 segundo.

Com essa alteração na arquitetura dos diretórios, foi possível obter uma redução de aproximadamente 93% no tempo de execução do código de reconhecimento, otimizando o desempenho do RECOFACE. É importante ressaltar que com a arquitetura de diretórios anterior, foi possível atestar o funcionamento do código, visto que ele reconheceu a imagem alvo dentro de um banco com 226 imagens em um tempo de aproximadamente 15 segundos.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Não é difícil imaginar situações em que a EAD necessite de uma melhor auditoria sobre a autenticidade dos trabalhos e autenticação de seus alunos. Um professor pode eventualmente ter que aplicar uma avaliação de forma remota para um aluno ou uma turma na Educação a Distância.

O estudo mostra que com a implementação de regras mais específicas de segurança da informação e através do uso de novas tecnologias, é possível auxiliar a Educação a Distância no monitoramento dos alunos, devido a capacidade de controle de acesso à plataforma.

Com a ferramenta é possível criar uma nova forma de ingresso dos alunos da Educação a Distância no AVA, contribuindo significativamente para a instituição que promove o curso. Além disso, colaborar com os alunos no que diz respeito ao monitoramento estudantil na plataforma de ensino.

Em relação a confiabilidade do método, o modo de reconhecimento deve seguir de forma rígida as regras no momento da obtenção das faces para cadastro e da face para reconhecimento, no qual o reconhecimento pode ser prejudicado por fatores biológicos e naturais, como o envelhecimento do estudante. Caso o estudante passe por um grande período de tempo matriculado no curso ou na instituição, uma atualização no cadastro do estudante poderá auxiliar na prevenção de problemas.

Considerando o melhor funcionamento da ferramenta, o aluno deve ser orientado como proceder da maneira correta no momento da captura da imagem, posicionando-se adequadamente para o registro da foto. Caso o reconhecimento seja negativo, o aluno não necessariamente irá ser desligado da plataforma de ensino, ele pode continuar seus estudos com o registro de uma observação nos relatórios do sistema, ou simplesmente repetir a ação.

Um produto de software não é algo tangível, e nem algo físico como outros produtos que estamos acostumados no nosso cotidiano (SOMMERVILE, 2007). Como discorre Martins (2007), que relata que o projeto é normalmente uma iteração, sendo que as primeiras versões dos *softwares* não são tão completas como aquelas desenvolvidas nas iterações mais recentes. Com isso, o protótipo precisa ser melhorado e atualizado para que possa ampliar a confiança no momento do reconhecimento.

Concluiu-se que as plataformas virtuais necessitam de melhorias na segurança da informação, para proporcionar um monitoramento adequado dos estudantes que utilizam essas plataformas, protegendo as informações de acessos indevidos. Essas ferramentas são úteis quando se precisa confirmar a presença de um aluno com algo mais forte do que uma senha. Como a disponibilização de cartões ou outros tipos de dispositivos são mais caros, a biometria facial se mostrou viável para a EAD, pois trabalha com dados transferidos pela internet, e a captura desses dados digitais em forma de imagem é feita por dispositivos comuns nos dispositivos computacionais atuais.

Como produto final, a pesquisa gerou um protótipo de *software* capaz de reconhecer padrões faciais, que disponibilizará uma forma de autenticação e de verificação de continuidade de permanência do aluno durante as atividades, possibilitando à instituição de ensino um controle de qualidade mais eficaz, sem que a flexibilidade e conveniência da Educação a Distância seja alterada.

Cabe destacar que a ferramenta não irá promover de forma isolada, o compromisso do aluno com o curso, e tampouco amplificar o aprendizado, mas as formas de uso do *software* pelos membros da Educação a Distância poderão contribuir com o acompanhamento e monitoramento desses estudantes.

Como trabalhos futuros a serem implementados no protótipo, podemos citar:

- Teste de Usabilidade: Testar a interface do protótipo, recolhendo informações sobre o uso, para melhorar a interação com o usuário.
- Realizar um estudo sobre a forma ideal para a captura das imagens para treinamento do protótipo.
- Realizar testes em larga escala, simulando de forma realística, o funcionamento do sistema, com o objetivo de validar o protótipo.
- Design Responsivo do protótipo: Adequar o protótipo para ser acessado por dispositivos móveis.

REFERÊNCIAS

- ABBAD, G. S. Educação a distância: o estado da arte e o futuro necessário. **Revista do Serviço Público**, v. 58, n. 3, p. 351-374, 2014.
- AHONEN, T.; HADID, A.; PIETIKÄINEN, M. Face recognition with local binary patterns. In: **European conference on computer vision**. Springer Berlin Heidelberg, 2004. p. 469-481.
- AHONEN, T.; HADID, A. PIETIKAINEN, M. Face description with local binary patterns: application to face recognition. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, Piscataway, v. 28, n. 12, p. 2037–2041, 2006.
- ALBERGARIA, E. T; SANTOS, K. C.L; JÚNIOR, M. S. F. A. Reconhecimento de faces utilizando programação genética. In: **Seminário de projeto e análise de algoritmos**. Universidade Federal de Minas Gerais, 2006.
- ALMEIDA, M. E. B. Tecnologia e educação a distância: abordagens e contribuições dos ambientes digitais e interativos de aprendizagem. In: **Reunião Anual da ANPED**, Poços de Caldas, MG, 2003.
- BERNARDI, M. F. **Proposta de um Modelo de Autenticação Segura para Acesso a Sites de Ensino a Distância Utilizando Biometria Facial**, Centro Estadual De Educação Tecnológica Paula Souza, Mestrado Em Tecnologia. 2007.
- BEUREN, I. M. **Como Elaborar Trabalhos Monográficos em Contabilidade**. 3. Ed. São Paulo: Atlas S. A., 2010.
- BIOSIG-ID, **BioSig-ID in the Education Industry**. Disponível em: <<https://www.biosig-id.com/industry/biosig-id-and-the-education-industry> >. Acesso em: 15 de junho de 2016.
- BORGES, L. E. **Python para desenvolvedores**. Novatec Editora, 2014.
- BRAGA, L. F. **Sistemas de reconhecimento facial**. Trabalho de Conclusão de Curso (Graduação em Engenharia Elétrica). Escola de Engenharia de São Carlos, Universidade de São Paulo. São Carlos, 2013.
- BRASIL. PRESIDÊNCIA DA REPÚBLICA. Decreto nº 5.602, de 6 de Dezembro de 2005. **Dispõe sobre a regulamentação do Programa de Inclusão Digital instituído pela Lei no 11.196**. Decreto on-line. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Decreto/D5602.htm>. Acesso em: 25 de maio de 2016.
- BRASIL. PRESIDÊNCIA DA REPÚBLICA. Decreto nº 6.300, de 12 de Dezembro de 2007. **Dispõe sobre o Programa Nacional de Tecnologia Educacional – ProInfo**. Decreto on-line. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato20072010/2007/Decreto/D6300.htm>. Acesso em: 25 de maio de 2016.

CASTANHA, D. P. G. D. **Auditoria em Segurança da Informação no Ambiente Uniriotec**. Trabalho de Conclusão de Curso – Universidade Federal do Estado do Rio de Janeiro, 2014. Disponível em: <<http://ftp.uniriotec.br/tcc/201406Possolo.pdf>> Acesso em: 27 de Agosto de 2016.

CASTILHO, J. M. **Estudo e implementação de técnicas de processamento de imagens aplicadas em reconhecimento de face**. Trabalho de Conclusão de Curso - Bacharel em Engenharia da Computação – Universidade Federal do Pará, 2012. Disponível em: <http://laps.ufpa.br/zampolo/ensino/tcc/tcc_janize.pdf >. Acesso em: 02 de junho de 2016.

Censo EAD.BR. **Relatório Analítico da Aprendizagem a Distância no Brasil 2012**, Curitiba: Ibpx, 2013.

CERT.br. **Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2015**, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. 2015. Disponível em: <<http://www.cert.br/stats/incidentes/2015-jan-dec/analise.html>> Acesso em 22 de Agosto de 2016.

CORDEIRO, F. R. **Desenvolvimento de um Mecanismo Semi-Supervisionado para Segmentação de Tumores em Imagens de Mamografia Digital**. Tese, Universidade Federal de Pernambuco, Centro de Informática, 2015.

DALL’OGLIO, P. **Php-programando com orientação a objetos**. Novatec Editora, 2015.

DINIZ, F.; NETO, F.; JÚNIOR, F.; FONTES, L. RedFace: Um Sistema de Reconhecimento Facial para Identificação de Estudantes em um Ambiente Virtual de Aprendizagem. **RENOTE - Revista Novas Tecnologias na Educação** (ISSN 1679-1916), CINTED-UFRGS, v. 10, n. 3, dez. 2012. Disponível em: <http://seer.ufrgs.br/index.php/renote/article/view/36403/23510>

DINIZ, F. A. **RedFace – Um Sistema de Reconhecimento de Expressões Faciais para Apoiar um Ambiente Virtual de Aprendizagem**. Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação – associação ampla entre a Universidade do Estado do Rio Grande do Norte e a Universidade Federal Rural do Semi-Árido, 2013a.

DINIZ, F.; NETO, F.; JÚNIOR, F.; FONTES, L. RedFace: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces: comparação com diferentes classificadores. **Revista Brasileira de Computação Aplicada** (ISSN 2176-6649), Passo Fundo, v. 5, n. 1, p. 42-54, abr. 2013b.

ENTTRY. **Face ID – Biometria Facial as a Service**. Disponível em: <<https://www.enttry.com.br/software/biometria-facial/faceid-biometria-facial/> >. Acesso em: 15 de junho de 2016.

FARINA, A. M. **Biomobile: sistema de identificação de usuários em dispositivos móveis na plataforma Android utilizando reconhecimento de faces a partir de**

vídeo. Universidade Estadual Paulista “Júlio de Mesquita Filho”, Dissertação de Mestrado, 2012.

FIGUEREDO, M. B. **Reconhecimento de faces aplicado ao problema de pessoas desaparecidas - Estudo de caso do Eigenface.** Dissertação (Mestrado) - SENAI CIMATEC, Salvador, 2011.

FIGORESE, M. **Uma proposta de autenticação de usuários para ensino a distância.** Dissertação de Mestrado em Ciência da Computação. Universidade Federal Do Rio Grande Do Sul. 2000.

FIGORESE, M.; TAROUCO, L. M. R. Uma Proposta de Autenticação de Usuários para Ensino a Distância. In: **18º Simpósio Brasileiro de Redes de Computadores.** Instituto de Informática da UFRGS. Porto Alegre - RS- Brasil, 2006.

FURLANO NETO, M.; BELLINETTI, G. **A assinatura digital como prova de autoria do documento eletrônico.** Disponível em: <<http://galileu.fundanet.br/revista/index.php/emtempo/article/view/20/44>>. Acesso em 08 de Maio de 2016.

GALEFFI, D. A. **O Ser-sendo da Filosofia.** Salvador: Edufba, 2001

GIAVAROTO, S. C. R.; SANTOS, G. R. dos. **“Backtrack Linux: Auditoria e Teste de Invasão em Redes de Computadores”.** São Paulo, Ciência Moderna Ltda, 2013.

GIL, A. C. **Métodos e técnicas em pesquisa social.** 5. ed. São Paulo: Atlas, 2010.

GILBERT, S.D. **How to be a Successful On-Line Student.** New York, McGraw-Hill, 2001. 74p.

GUIMARÃES, R. M. **Desenvolvimento de um Protótipo de Software de Reconhecimento Facial de Tempo Real para Registro Eletrônico de Ponto em Ambientes Indoor com Utilização do Dispositivo KINECT.** Dissertação submetida ao Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC, Belo Horizonte, 2015. Disponível em: <<http://www.fumec.br/revistas/sigc/article/view/3037/1878>> Acesso em: 21 de agosto de 2016.

HANZRA, B. S. **Face Recognition using Python and OpenCV, 2015.** Disponível em: <http://hanzratech.in/2015/02/03/face-recognition-using-opencv.html> Acesso em: 21 de agosto de 2016.

INEP. (2013) **Censo da educação superior: 2012 – resumo técnico.** – Brasília: Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, 2013. Disponível em: <http://download.inep.gov.br/download/superior/censo/2011/resumo_tecnico_censo_educacao_superior_2011.pdf> Acesso em: 18 de julho de 2016.

JAIN, K. A.; ROSS, A.; PRABHAKAR, S. **An introduction to biometric recognition**. Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, v. 14, n. 1, January 2004.

KAZIENKO, J. F. **Assinatura Digital de Documentos Eletrônicos Através da Impressão Digital**. Dissertação (Mestrado) - Universidade Federal de Santa Catarina, fev. 2003.

KINUTA, C; MOLINA, D; DORNELES, E. G; GRECCHI, F. S; DIAS, G. T; SANTANA, J; FERNANDES JÚNIOR, O. O. Estudo comparativo de algoritmos para reconhecimento facial. In: **SEGeT – Simpósio de excelência em gestão e tecnologia**. Universidade IMES, São Caetano do Sul, 2006. Disponível em: <http://www.aedb.br/seget/arquivos/artigos06/916_Copia%20de%20Artigo%20Comparativo%20Facial.pdf> Acesso em: 21 ago. 2016.

KSHIRSAGAR, V. P.; BAVISKAR, M. R.; GAIKWAD, M. E. Face recognition using Eigenfaces. **Computer Research and Development (ICCRD), 3rd International Conference on**, vol. 2, no., pp. 302-306, 11-13, 2011.

MARAIS, E.; ARGLES D.; VON SOLMS B. Security issues specific to e-assessments, **8th Annual Conference on WWW Applications**, 2006.

MARTINS, J. C. C. **Técnicas para gerenciamento de projetos de software**. Brasport, 2007.

MARTINS, T. S.; LUCAS, E. R. O. Os programas de inclusão digital do Governo Federal sob a óptica da competência informacional. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, v. 5, n. 1, 2012.

MASCARENHAS, S. A. (Org.) **Metodologia científica**. São Paulo: Pearson, 2012.

MELLO, C. M.; BERGAMO, E. A.; MELLO, R. A. **Políticas Públicas de Educação: PROUNI, Conselhos Escolares e Educação a Distância**. Curitiba: Camões, 2009.

MENESES, P. R. et al. Introdução ao processamento de imagens de sensoriamento remoto. **Brasília: UNB/CNPq**, 2012.

MONACO, V. **Moodle BioAuth Plugin. 2013**. Disponível em: <<http://vmonaco.com/moodle-bioauth-plugin/>>. Acesso em: 15 de junho de 2016.

MORAES, J. L. **Controle de acesso baseado em biometria facial**, Dissertação de mestrado, Pós-Graduação em Informática do Centro Tecnológico da Universidade Federal do Espírito Santo, Vitória, 2010.

MORAIS, M. A. C. **A importância da educação profissional na modalidade de educação a distância para o desenvolvimento territorial**, Tese apresentada ao Programa de Pós-Graduação em Geografia do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho” – UNESP – Campus Rio Claro, RIO CLARO, 2015. Disponível

em:<http://repositorio.unesp.br/bitstream/handle/11449/133983/morais_mac_dr_rcla.pdf?sequence=3&isAllowed=y> Acesso em: 21 de agosto de 2016.

NAKAMURA, E. T.; GEUS, P. L. de. “**Segurança de Redes em Ambientes Cooperativos**”. Rio de Janeiro, Novatec Editora Ltda, 2010.

NASCIMENTO, V. **Implementação de um sistema de identificação facial utilizando Linux embarcado**, Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de São Carlos, 2015.

NEVES, J. L. Pesquisa qualitativa: características, usos e possibilidades. **Caderno de Pesquisa em administração**. FEA-USP. São Paulo, v. 1, n. 3, 2º sem, 1996.

NIEDERAUER, J. **Desenvolvendo websites com PHP**. São Paulo: Novatec, 2004.

NUNAN, A. E.; COSTA FILHO, M. J. M.; LIMA, A. A. Implantação da segurança na gestão da informação na administração pública: um estudo de caso no Tribunal de Contas do Estado do Amazonas. **Revista do Serviço Público**, v. 67, n. 1, p. 110-131, 2016.

OJALA, T.; PIETIKÄINEN, M.; HARWOOD, D. A comparative study of texture measures with classification based on feature distributions. **Pattern Recognition**, Amsterdam, v. 29, n. 1, p. 51–59, 1996.

OKABE, R. K.; CARRO, S. A. Reconhecimento facial em imagens capturadas por câmeras digitais de rede. In: **Colloquium Exactarum**. 2015. p. 106-119.

OLIVEIRA, A. E.; SILVA, E. A educação a distância e sua contribuição na inclusão social. **Cadernos Zygmunt Bauman**, v. 5, n. 10, 2016.

OPENCV, **Open Source Computer Vision Library - Cascade Classification**, 2016a. Disponível em:
<http://docs.opencv.org/2.4/modules/objdetect/doc/cascade_classification.html>
Acesso em: Julho 2016.

OPENCV, **Open Source Computer Vision Library - Face Recognition with OpenCV**, 2016b. Disponível em:
<http://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html#face-recognition> Acesso em 26 de Julho de 2016.

PACHECO, J. A. **Currículo**: Teoria e Práxis. Portugal: Porto, 1996

PALLOFF, R. M.; PRATT, K. **O aluno virtual**: um guia para trabalhar com estudantes on-line. Porto Alegre: Artmed, 2004.

PATIN, F. “**An Introduction to digital image processing**”. Disponível em:
<<http://article.programmersheaven.com/Patin/ImageProc.pdf>>. Acesso em: 09 de maio de 2016.

PENTEADO, B. E. **Autenticação biométrica de usuários em sistemas de e-learning baseada em reconhecimento de faces a partir de vídeo**. Dissertação de Mestrado em Ciência da Computação. UNESP, São José do Rio Preto, 2009.

PENTEADO, B. E.; MARANA, A. N. A Video-Based Biometric Authentication for ELearning Web Applications. In: **Eleventh International Conference on Enterprise Information Systems**, ICEIS 2008, 2009, Milão. LNBIP - Lecture Notes on Business Information Processing. Berlin: Springer-Verlag, v. 24. p. 770-779, 2009.

PEREIRA, A. **Ambientes Virtuais de Aprendizagem**: em diferentes contextos. Rio de Janeiro: Ciência Moderna Ltda, 2007.

PINHEIRO, P. P. Aspectos legais da biometria. **Revista TI Inside**, São Paulo, p. 30, nov. 2007.

PRESSMAN, R. S. **Engenharia de software**. São Paulo: Makron Books, 1995.

PRESMAN, R. S. **Engenharia de Software**. 5.ed. Rio de Janeiro: McGraw-Hill, 2002.

RABUZIN, K.; BACA, M.; SAJKO, M. E-learning: Biometrics as a Security Factor. In: **2006 International Multi-Conference on Computing in the Global Information Technology-(ICCGI'06)**. IEEE, 2006. p. 64-64.

RAMOS, A. Security Officer: guia oficial para formação de gestores em segurança da informação. **Porto Alegre: Zouk**, 2006.

ROLIM, A. L.; BEZERRA E. P. Um sistema de identificação automática de faces para um ambiente virtual de ensino e aprendizagem. In: **Companion Proceedings of the XIV Brazilian Symposium on Multimedia and the Web**, 2008.

ROLIM, A. L. **Um sistema de identificação automática de faces para Ambientes Virtuais de Aprendizagem**. Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal da Paraíba, 2009.

SANTOS, C. N. dos. **Aprendizado de máquina na identificação de sintagmas nominais**: o caso do português brasileiro. Rio de Janeiro, 2005. Disponível em: <<http://www.linguateca.pt/Repositorio/DissertacaoCicero2005.pdf>> Acesso em: 26 de maio de 2016.

SCHWABER, K., BEEDLE, M., **Agile Software Development With Scrum**, Prentice Hall, 2002.

SILVA, C. R. C. Ambientes virtuais de aprendizagem: avaliação de usabilidade e interatividade na perspectiva de docentes e discentes. **SIED: EnPED-Simpósio Internacional de Educação a Distância e Encontro de Pesquisadores em Educação a Distância**, 2016.

SILVA, J. C. **Aplicação de sistemas imunológicos artificiais para biometria facial**: reconhecimento de identidade baseado nas características de padrões

binários. 2015. 204 p. Tese (doutorado) - Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Engenharia, 2015. Disponível em: <<http://hdl.handle.net/11449/127901>>. Acesso em 21 de agosto de 2016.

SILVA, M. A. A. **Extração e Comparação de Características Locais para o Reconhecimento Facial por Meio de Retratos Falados**. Tese de Doutorado. Universidade Federal de Ouro Preto. 2014.

SOMMERVILLE, I. **Engenharia de software**. 6° ed. Tradução Maurício de Andrade. São Paulo: Ed Addison-Wesley, 2003.

SOMMERVILLE, I. **Engenharia de software**. São Paulo: Addison-Wesley, 2007.

SUNG, K.K., POGGIO, T. **Example – based Learning for View – based Human Face Detection**. Massachusetts: Massachusetts Institute of Technology, December 1994.

TAVARES, A. L.; ECKEL, A. P.; SCARPA, C.; VENDRAME, Z. R. **Engenharia de Software: uma visão geral**. Disponível em: <http://www.joinville.udesc.br/portal/professores/claudinei/materiais/SOFT_VISAO_GERAL.pdf>. Acesso em: 29 Maio de 2016.

TOLENTINO, G. C. A.; TSUKAMOTO, D. B.; NOMURA, S. Estudo de caso: Utilização do Arduino para um Sistema de Controle remoto de dispositivos via internet. In: **XI CEEL - Conferencia de Estudos em Engenharia Elétrica**, Uberlândia MG, 2013. Disponível em: <http://www.ceel.eletrica.ufu.br/artigos2013/ceel2013_052.pdf> Acesso em 22 de julho 2016.

VERGARA, S. C. Começando a definir a metodologia. In: VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 10. Ed. São Paulo: Atlas, 2009.

VIOLA, P.; JONES, M. Rapid object detection using a boosted cascade of simple features. In: **Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on**. IEEE, 2001. p. I-511-I-518 vol. 1.

VIOLA, P. A.; JONES M. J. Robust real-time object detection, **International Journal of Computer Vision**, 57(2): 137-154, 2004.

XIANG, C. Feature Extraction For Face Recognition, **Engineering Research**, v. 21, n. 2, 2006. Disponível em: <http://www.eng.nus.edu.sg/EResnews/0606/sf/sf8.html> Acesso em: 21 de agosto de 2016.

ZELINSKY, A. Learning OpenCV---Computer Vision with the OpenCV Library (Bradski, GR et al.; 2008)[On the Shelf]. **Robotics & Automation Magazine, IEEE**, v. 16, n. 3, p. 100-100, 2009.

APÊNDICE A – QUESTIONÁRIO APLICADO NA PESQUISA

PESQUISA SOBRE AMBIENTES VIRTUAIS DE APRENDIZAGEM (AVA) COM O USO DE BIOMETRIA FACIAL NA EDUCAÇÃO A DISTÂNCIA.

O presente questionário é parte integrante de pesquisa do Mestrado Profissional em Tecnologia e Gestão em Educação a Distância da UFRPE. Desta forma, convidamos você a responder este questionário que tem como objetivo coletar dados para a pesquisa “Ambientes Virtuais de Aprendizagem com Biometria Facial”, conduzido pelo pesquisador Robson Almeida Borges de Freitas. Antecipadamente queremos agradecer por sua contribuição para a continuidade deste trabalho.

*Obrigatório

1 - Qual a sua experiência com Educação a Distância (EAD)? *

- Estudante
- Professor Conteudista
- Professor Pesquisador
- Tutor a Distância
- Tutor Presencial
- Coordenador

2 - Você considera os Ambientes Virtuais de Aprendizagem (AVA) propícios a algum tipo de fraude? *

- Sim
- Não

3 - Você considera importante o desenvolvimento e o uso de novas ferramentas tecnológicas para melhoria da EAD? *

- Sim
- Não

4 - Se tratando da forma do estudante logar (entrar) na plataforma de estudo, você considera o método USUÁRIO/SENHA suficiente para garantir o monitoramento do aluno e garantir as horas de estudo? *

- Sim
- Não

5 - Métodos biométricos são utilizados para segurança em vários Sistemas de Informação, por exemplo, são utilizados no processo

eleitoral brasileiro. A biometria seria uma forma de melhorar o monitoramento do estudante na Educação a Distância? *

- Sim
- Não

6 - Você conhece algum AVA que forneça métodos biométricos de monitoramento estudantil? *

- Sim
- Não

Se sim, Qual?

7 - A Biometria Facial como forma de login nas plataformas melhoraria o monitoramento do aluno na EAD? *

- Sim
- Não

Por quê?

APÊNDICE B – Códigos do protótipo

Arquivo Index.php

```

<script type='text/javascript' src='webcam.js' charset="UTF-8"></script>
    <script type='text/javascript' charset="UTF-8">
        //Configurando o arquivo que vai receber a imagem
        webcam.set_api_url('upload.php');
        //Setando a qualidade da imagem (1 - 100)
        webcam.set_quality(90);
        //Habilitando o som de click
        webcam.set_shutter_sound(true);
        //Definindo a função que será chamada após o
termino do processo
        webcam.set_hook('onComplete',
'my_completion_handler');
        //Função para tirar snapshot
        function take_snapshot() {
            if(numero == 1){alert('Para realizar o
cadastro é preciso a captura de 3 fotos do seu rosto!');};
            if (numero<4) {

document.getElementById('upload_results').innerHTML =
'<center><h1>Enviando...</h1></center>';
                webcam.snap();
                alert('A '+numero+'ª foto foi
tirada com sucesso!');
                    numero++;}
                else { alert('A operação foi realizada
com SUCESSO! O RecoFace realizou a captura das fotos do seu
rostos! Caso queira realizá-la novamente, aperte o botão:
CADASTRAR A FACE');
                    numero = 1;};
            };
        //Função callback que será chamada após o final do
processo
        function my_completion_handler(msg) {
            if (msg.match(/(http\:\/\/\/\S+)/)) {
                var htmlResult = '<center><h1>Enviado com
Sucesso!</h1></center>';
                htmlResult += '<center></center>';
document.getElementById('upload_results').innerHTML =
htmlResult;
                    webcam.reset();
                }
            else {
                alert('PHP Erro:' + msg);
            }
        }
    </script>

```

```

        };
        function redirecionar(){
            location.href = "inicioreco.php";
        }
    </script>
<?php
    header('Content-Type: text/html; charset=utf-8');
    if (isset($_COOKIE['usuario'])) {
        $login_cookie = $_COOKIE['usuario'];
        $contador = $_COOKIE['contador'];
    }
    if(isset($login_cookie)){
        echo"<center><img src='logo.jpg' /></center>";
        echo"<center><h2>Bem-Vindo,
$login_cookie</h2></center>";
        echo"<center><h2>Essas informações <font
color='red'>PODEM</font> ser acessadas por
você</h2></center>";
        echo"<!DOCTYPE html>
<html>
    <head>
        <title>Captura de imagens do RECOFACE</title>
        <meta charset='UTF-8'>
        <meta name='viewport' content='width=device-width'>
        <script>var numero = 1;</script>
        <style type='text/css'>
            .botaomenor{
                font-size:11px;
                font-family:Verdana,Helvetica;
                font-weight:bold;
                color:black;
                background:#638cb5;
                border:2px;
                width:80px;
                height:20px;
                margin:2px;
                border-radius: 5px;
            }
            .botaomaior{
                font-size:11px;
                font-family:Verdana,Helvetica;
                font-weight:bold;
                color:black;
                background:#638cb5;
                border:2px;
                width:400px;
                height:20px;
                margin:2px;
                border-radius: 5px;
            }
            .botaomedio{
                font-size:11px;

```


Arquivo tela_inicio_login_recoface.html

```
<!DOCTYPE html>
<html>
<head>
  <title>TELA DE LOGIN DO RECOFACE</title>
  <meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
</head>
<body>
<center><img src='logo.jpg' /></center> <br>
<form method="POST" action="validar.php">
  <center><h2><label>Usuário:</label><input type="text"
name="usuario" id="usuario" maxlength="50"></h2></center><br>

  <center><h2><label>Senha:</label><input type="password"
name="senha" id="senha" maxlength="50"></h2></center><br>

  <center><h2><input type="submit" value="entrar" id="entrar"
name="entrar"></h2></center><br>
  <center><h2><a
href="cadastro_recoface_tela_inicial.html">Cadastre-
se</a></h2></center>
</form>
</body>
</html>
```

Arquivo cadastro_recoface_tela_inicial.html

```
<html>
  <head>
    <title> Cadastro de Usuário - RECOFACE </title>
    <meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
  </head>
  <body>
    <center><img src='logo.jpg' /></center> <br>
    <form method="POST"
action="cadastro_no_banco_usuario.php">
      <center><h2><label>Usuário:</label><input
type="text" name="usuario" id="usuario"></h2></center><br>
      <center><h2><label>Senha:</label><input
type="password" name="senha" id="senha"></h2></center><br>
      <center><h2><input type="submit"
value="Cadastrar" id="cadastrar"
name="cadastrar"></h2></center>
    </form>
  </body>
</html>
```

Arquivo cadastro_no_banco_usuario.php

```

<?php
header('Content-Type: text/html; charset=utf-8');
$login = $_POST['usuario'];
$senha = MD5($_POST['senha']);
$connect = mysql_connect('localhost','root','');
$db = mysql_select_db('recoface_login_php');
$query_select = "SELECT usuario FROM usuarios WHERE usuario =
'$login'";
$select = mysql_query($query_select,$connect);
$array = mysql_fetch_array($select);
$logarray = $array['usuario'];

    if($login == "" || $login == null){
        echo"<script language='javascript'
type='text/javascript'>alert('O campo login deve ser
preenchido');window.location.href='cadastro_recoface_tela_inic
ial.html';</script>";
    }else{
        if($logarray == $login){

            echo"<script language='javascript'
type='text/javascript'>alert('Esse login já
existe');window.location.href='cadastro_recoface_tela_inicial.
html';</script>";
            die();

        }else{
            $query = "INSERT INTO usuarios (usuario,senha)
VALUES ('$login','$senha)";
            $insert = mysql_query($query,$connect);

            if($insert){
                echo"<script language='javascript'
type='text/javascript'>alert('Usuário cadastrado com
sucesso!');window.location.href='tela_inicio_login_recoface.ht
ml'</script>";
            }else{
                echo"<script language='javascript'
type='text/javascript'>alert('Não foi possível cadastrar esse
usuário');window.location.href='cadastro_recoface_tela_inicial
.html'</script>";
            }
        }
    }
?>

```

Arquivo validar.php

```
<?php
    $login = $_POST['usuario'];
    $entrar = $_POST['entrar'];
    $senha = md5($_POST['senha']);
    $connect = mysql_connect('localhost','root','');
    $db = mysql_select_db('recoface_login_php');
    $contador = 1;
        if (isset($entrar)) {

            $verifica = mysql_query("SELECT * FROM usuarios
WHERE usuario = '$login' AND senha = '$senha'") or die("erro
ao selecionar");
                if (mysql_num_rows($verifica)<=0){
                    echo"<script language='javascript'
type='text/javascript'>alert('Login e/ou senha
incorretos');window.location.href='tela_inicio_login_recoface.
html!';</script>";
                        die();
                    }else{
                        setcookie("usuario",$login);
                        setcookie("contador",$contador);
                        header("Location:index.php");
                    }
                }
    }
?>
```

Arquivo upload.php

```

<?php
    session_start();
    header('Content-Type: text/html; charset=utf-8');
    if (isset($_COOKIE['usuario'])) {
        $login_cookie = $_COOKIE['usuario'];
        $contador = $_COOKIE['contador'];
        if ($contador == 4) {
            $contador = 1;
        }
    }

    $connect = mysql_connect('localhost','root','');
    $db = mysql_select_db('recoface_login_php');
    $query_select = "SELECT id FROM usuarios WHERE
usuario = '$login_cookie'";
    $consulta = mysql_query($query_select,$connect);
    $idusuario = mysql_fetch_assoc($consulta);
    $uploadDir = 'reconhecimento/'.$login_cookie.'/uploads';

    if(!is_dir($uploadDir)){
        if (!mkdir($uploadDir, 0777, true)) {
            print "ERRO: Não foi possível criar o diretório";
        }
    }

    if(!is_writable($uploadDir)){
        chmod($uploadDir, 0777);
    }
    $name =
$uploadDir.'/'.$login_cookie.'_'.$contador.'.'.$idusuario['id']
].'usuario';
    $file = file_put_contents($name,
file_get_contents('php://input'));
    if (!$file) {
        print "ERRO: Falha de escrita para o arquivo [$name],
É necessário dar permissão de escrita na pasta
[$uploadDir]\n";
        exit();
    }
    if ($contador <= 3) {
        $contador = $contador + 1;
        setcookie('contador',$contador);
    }
    print
'http://'.$_SERVER['HTTP_HOST'].dirname($_SERVER['REQUEST_URI']
)].'/'.$name;
?>

```

Arquivo chamar_yale.php

```

<?php
header('Content-Type: text/html; charset=utf-8');
    if (isset($_COOKIE['usuario'])) {
        $login_cookie = $_COOKIE['usuario'];
        $contador = $_COOKIE['contador'];
    }
        if(isset($login_cookie)){
            echo"<center><img src='logo.jpg' /></center>";
            echo"<center><h2>Bem-Vindo,
$login_cookie</h2></center>";
            echo"<center><h2>Essas informações <font
color='red'>PODEM</font> ser acessadas por
você</h2></center>";
            echo"<center><h4>";system("face_recognizer.py");
echo"</h4></center>";
        }else{
            echo"<center><img src='logo.jpg' /></center>
<br>";
            echo"<center><h2>Bem-Vindo,
convidado!</h2></center> <br>";
            echo"<center><h2>Essas informações <font
color='red'>NÃO PODEM</font> ser acessadas por você, DIRIJA-SE
À TELA DE LOGIN DO RECOFACE!</h2></center>";
            echo"<br><center><h2><a
href='tela_inicio_login_recoface.html'>Faça Login</a> Para ler
o conteúdo</h2></center>";
        }
?>

```

Arquivo inicioreco.php

```

<script type='text/javascript' src='webcam.js' charset='UTF-8'></script>
    <script type='text/javascript' charset='UTF-8'>
        //Configurando o arquivo que vai receber a imagem
        webcam.set_api_url('guardarreco.php');
        //Setando a qualidade da imagem (1 - 100)
        webcam.set_quality(90);
        //Habilitando o som de click
        webcam.set_shutter_sound(true);
        //Definindo a função que será chamada após o
termino do processo
        webcam.set_hook('onComplete',
'my_completion_handler');
        //Função para tirar snapshot
        function take_snapshot() {
            alert('Para realizar o reconhecimento devemos
capturar a foto da sua face! Tenha cuidado com a iluminação e
o uso de utensílios como óculos e chapéus, tentando reproduzir
a imagem o mais parecido possível com a da captura no
cadastro!');

document.getElementById('upload_results').innerHTML =
'<center><h1>Enviando...</h1></center>';
            webcam.snap();
            alert('A foto foi tirada com
sucesso!');
        };
        //Função callback que será chamada após o final do
processo
        function my_completion_handler(msg) {
            if (msg.match(/(http\:\/\/\/\S+)/)) {
                var htmlResult = '<center><h1>Enviado com
Sucesso!</h1></center>';
                htmlResult += '<center></center>';
                htmlResult += '<center><h1>Caro Usuário,
sua foto foi capturada com sucesso! Em seguida faça o
reconhecimento apertando RECONHECER.</h1></center>';

document.getElementById('upload_results').innerHTML =
htmlResult;

                webcam.reset();
            }
            else {
                alert('PHP Erro: ' + msg);
            }
        };
    </script>
<?php

```

```

header('Content-Type: text/html; charset=utf-8');
if (isset($_COOKIE['usuario'])) {
    $login_cookie = $_COOKIE['usuario'];
    $contador = $_COOKIE['contador'];
}
if(isset($login_cookie)){
    echo"<center><img src='logo.jpg' /></center>";
    echo"<center><h2>Bem-Vindo,
$login_cookie</h2></center>";
    echo"<center><h2>Essas informações <font
color='red'>PODEM</font> ser acessadas por
você</h2></center>";
    echo"<!DOCTYPE html>
<html>
<head>
<title>Captura de imagens do RECOFACE</title>
<meta charset='UTF-8'>
<meta name='viewport' content='width=device-width'>
<style type='text/css'>
    .botaomenor{
    font-size:11px;
    font-family:Verdana,Helvetica;
    font-weight:bold;
    color:black;
    background:#638cb5;
    border:2px;
    width:80px;
    height:20px;
    margin:2px;
    border-radius: 5px;
    }
    .botaomaior{
    font-size:11px;
    font-family:Verdana,Helvetica;
    font-weight:bold;
    color:black;
    background:#638cb5;
    border:2px;
    width:400px;
    height:20px;
    margin:2px;
    border-radius: 5px;
    }
    .botaomedio{
    font-size:11px;
    font-family:Verdana,Helvetica;
    font-weight:bold;
    color:black;
    background:#638cb5;
    border:2px;
    width:130px;

```


Arquivo guardarreco.php

```

<?php
    session_start();
    header('Content-Type: text/html; charset=utf-8');
    if (isset($_COOKIE['usuario'])) {
        $login_cookie = $_COOKIE['usuario'];
    }

    $connect = mysql_connect('localhost','root','');
    $db = mysql_select_db('recoface_login_php');
    $query_select = "SELECT id FROM usuarios WHERE
usuario = '$login_cookie'";
    $consulta = mysql_query($query_select,$connect);
    $idusuario = mysql_fetch_assoc($consulta);
    $uploadDir = 'reconhecimento/'.$login_cookie;

    if(!is_dir($uploadDir)){
        if (!mkdir($uploadDir, 0777, true)) {
            print "ERRO: Não foi possível criar o diretório";
        }
    }
    if(!is_writable($uploadDir)){
        chmod($uploadDir, 0777);
    } else {
        $arquivo_origem = 'reconhecimento.py';
        $arquivo_destino =
'reconhecimento/'.$login_cookie.'/reconhecimento.py';
        copy($arquivo_origem, $arquivo_destino);
        $arquivo_origem2 = 'chamar_python.php';
        $arquivo_destino2 =
'reconhecimento/'.$login_cookie.'/chamar_python.php';
        copy($arquivo_origem2, $arquivo_destino2);
        $arquivo_origem3 =
'haarcascade_frontalface_default.xml';
        $arquivo_destino3 =
'reconhecimento/'.$login_cookie.'/haarcascade_frontalface_defa
ult.xml';
        copy($arquivo_origem3, $arquivo_destino3);
    }
    $name =
$uploadDir.'/'.$login_cookie.'.'.$idusuario['id'].'usuario';
    $file = file_put_contents($name,
file_get_contents('php://input'));
    if (!$file) {
        print "ERRO: Falha de escrita para o arquivo [$name],
É necessário dar permissão de escrita na pasta
[$uploadDir]\n";
        exit();
    }
}
Print'http://'.$_SERVER['HTTP_HOST'].dirname($_SERVER['REQUEST
_URI'])..'/'.$name;?>

```

Arquivo chamar_python.php

```

<?php
header('Content-Type: text/html; charset=utf-8');
    if (isset($_COOKIE['usuario'])) {
        $login_cookie = $_COOKIE['usuario'];
        $contador = $_COOKIE['contador'];
    }
    $connect = mysql_connect('localhost','root','');
    $db = mysql_select_db('recoface_login_php');
    $query_select = "SELECT id FROM usuarios WHERE usuario =
'$login_cookie'";
    $select = mysql_query($query_select,$connect);
    $array = mysql_fetch_array($select);
    $ident = $array['id'];
date_default_timezone_set('America/Sao_Paulo');
    $pega_data = date('Y-m-d H:i:s');
    if(isset($login_cookie)){
        echo"<center><img src='../../logo.jpg'
/></center>";
        echo"<center><h2>Bem-Vindo,
$login_cookie</h2></center>";
        echo"<center><h2>Essas informações <font
color='red'>PODEM</font> ser acessadas por
você</h2></center>";
        echo"<center><h4>"; $colocarbanco =
system("reconhecimento.py");
        $query = "INSERT INTO registro
(id_reg, registros, datahora) VALUES
('$ident','$colocarbanco','$pega_data')";
        $insert =
mysql_query($query,$connect);
        echo mysql_error();
        if($insert){
            echo"<script language='javascript'
type='text/javascript'>alert('Reconhecimento cadastrado com
sucesso!');window.location.href='http://162.243.44.232/moodle/
'</script>";}else{echo"<script language='javascript'
type='text/javascript'>alert('Não foi possível cadastrar o
reconhecimento desse usuário, Por Favor, Tente
Novamente!')</script>";
            echo"</h4></center>";}}else{
            echo"<center><img src='logo.jpg' /></center>
<br>";echo"<center><h2>Bem-Vindo, convidado!</h2></center>
<br>";echo"<center><h2>Essas informações <font color='red'>NÃO
PODEM</font> ser acessadas por você, DIRIJA-SE À TELA DE LOGIN
DO RECOFACE!</h2></center>";
            echo"<br><center><h2><a
href='tela_inicio_login_recoface.html'>Faça Login</a> Para ler
o conteúdo</h2></center>";
        }?>

```

Arquivo reconhecimento.py

```

#!C:\Python27\python.exe
# coding: utf-8
# Import the required modules
import cv2, os
import numpy as np
from PIL import Image

# For face detection we will use the Haar Cascade provided by
OpenCV.
cascadePath = "haarcascade_frontalface_default.xml"
faceCascade = cv2.CascadeClassifier(cascadePath)

# For face recognition we will use the LBPH Face Recognizer
recognizer = cv2.createLBPHFaceRecognizer()

# pasta(path) das imagens para treinamento
path = 'uploads'
def get_images_and_labels(path):
    image_paths = [os.path.join(path, f) for f in
os.listdir(path) if f.endswith('usuario')]
    # images will contains face images
    images = []
    # labels will contains the label that is assigned to the
image
    labels = []
    for image_path in image_paths:
        # Read the image and convert to grayscale
        image_pil = Image.open(image_path).convert('L')
        # Convert the image format into numpy array
        image = np.array(image_pil, 'uint8')
        # Get the label of the image
        nbr =
int(os.path.split(image_path)[1].split(".")[1].replace("usuari
o", ""))
        # Detect the face in the image
        faces = faceCascade.detectMultiScale(image)
        # If face is detected, append the face to images and
the label to labels
        for (x, y, w, h) in faces:
            images.append(image[y: y + h, x: x + w])
            labels.append(nbr)
            cv2.imshow("Adicionando as faces para o
treinamento...", image[y: y + h, x: x + w])
            cv2.waitKey(50)
    # return the images list and labels list
    return images, labels
# Call the get_images_and_labels function and get the face
images and the
# corresponding labels

```

```

images, labels = get_images_and_labels(path)
cv2.destroyAllWindows()

# Perform the training
recognizer.train(images, np.array(labels))
# pasta(path) das imagens para reconhecimento
path = os.getcwd()

image_paths = [os.path.join(path, f) for f in os.listdir(path)
if f.endswith('usuario')]
for image_path in image_paths:
    predict_image_pil = Image.open(image_path).convert('L')
    predict_image = np.array(predict_image_pil, 'uint8')
    faces = faceCascade.detectMultiScale(predict_image)
    for (x, y, w, h) in faces:
        nbr_predicted, conf =
recognizer.predict(predict_image[y: y + h, x: x + w])
        nbr_actual =
int(os.path.split(image_path)[1].split(".")[1].replace("usuari
o", ""))
        if nbr_actual == nbr_predicted:
            print "Usuário de identificação-{}, a face foi
reconhecida com confiança de: {}".format(nbr_actual, conf)
        else:
            print "{} Face Incompatível com
{}".format(nbr_actual, nbr_predicted)
            cv2.imshow("Reconhecendo a Face", predict_image[y: y +
h, x: x + w])
            cv2.waitKey(1000)

```

Arquivo face_recognizer.py

```

#!C:\Python27\python.exe

# Import the required modules
import cv2, os
import numpy as np
from PIL import Image

# For face detection we will use the Haar Cascade provided by
OpenCV.
cascadePath = "haarcascade_frontalface_default.xml"
faceCascade = cv2.CascadeClassifier(cascadePath)

# For face recognition we will use the LBPH Face Recognizer
recognizer = cv2.createLBPHFaceRecognizer()

def get_images_and_labels(path):
    # Append all the absolute image paths in a list
    image_paths
    # We will not read the image with the .sad extension in
    the training set
    # Rather, we will use them to test our accuracy of the
    training
    image_paths = [os.path.join(path, f) for f in
os.listdir(path) if not f.endswith('.sad')]
    # images will contains face images
    images = []
    # labels will contains the label that is assigned to the
    image
    labels = []
    for image_path in image_paths:
        # Read the image and convert to grayscale
        image_pil = Image.open(image_path).convert('L')
        # Convert the image format into numpy array
        image = np.array(image_pil, 'uint8')
        # Get the label of the image
        nbr =
int(os.path.split(image_path)[1].split(".")[0].replace("subjec
t", ""))
        # Detect the face in the image
        faces = faceCascade.detectMultiScale(image)
        # If face is detected, append the face to images and
        the label to labels
        for (x, y, w, h) in faces:
            images.append(image[y: y + h, x: x + w])
            labels.append(nbr)
            cv2.imshow("Adding faces to traning set...",
image[y: y + h, x: x + w])
            cv2.waitKey(50)
    # return the images list and labels list

```

```

    return images, labels

# Path to the Yale Dataset
path = 'yalefaces'
# Call the get_images_and_labels function and get the face
images and the
# corresponding labels
images, labels = get_images_and_labels(path)
cv2.destroyAllWindows()

# Perform the training
recognizer.train(images, np.array(labels))

# Append the images with the extension .sad into image_paths
image_paths = [os.path.join(path, f) for f in os.listdir(path)
if f.endswith('.sad')]
for image_path in image_paths:
    predict_image_pil = Image.open(image_path).convert('L')
    predict_image = np.array(predict_image_pil, 'uint8')
    faces = faceCascade.detectMultiScale(predict_image)
    for (x, y, w, h) in faces:
        nbr_predicted, conf =
recognizer.predict(predict_image[y: y + h, x: x + w])
        nbr_actual =
int(os.path.split(image_path)[1].split(".")[0].replace("subject", ""))
        if nbr_actual == nbr_predicted:
            print "{} is Correctly Recognized with confidence
{}".format(nbr_actual, conf)
        else:
            print "{} is Incorrect Recognized as
{}".format(nbr_actual, nbr_predicted)
            cv2.imshow("Recognizing Face", predict_image[y: y + h,
x: x + w])
            cv2.waitKey(1000)

```

SQL para criação do Banco de Dados

```
-- phpMyAdmin SQL Dump
-- version 4.0.4
-- http://www.phpmyadmin.net
-- Base de Dados: `recoface_login_php`
CREATE DATABASE IF NOT EXISTS `recoface_login_php` DEFAULT
CHARACTER SET utf8 COLLATE utf8_general_ci;
USE `recoface_login_php`;

-----

--
-- Estrutura da tabela `registro`
--

CREATE TABLE IF NOT EXISTS `registro` (
  `registros` varchar(300) NOT NULL,
  `datahora` datetime NOT NULL,
  `id_reg` int(10) unsigned NOT NULL,
  KEY `fk_id_reg` (`id_reg`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- Extraindo dados da tabela `registro`
-----
-- Estrutura da tabela `usuarios`

CREATE TABLE IF NOT EXISTS `usuarios` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `usuario` varchar(50) NOT NULL,
  `senha` varchar(50) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `usuario` (`usuario`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 AUTO_INCREMENT=31 ;

--
-- Limitadores para a tabela `registro`
--

ALTER TABLE `registro`
  ADD CONSTRAINT `fk_id_reg` FOREIGN KEY (`id_reg`) REFERENCES
`usuarios` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION;
```