CENTRO UNIVERSITÁRIO DE JOÃO PESSOA - UNIPÊ
PRÓ-REITORIA DE ENSINO DE GRADUAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

JOÃO RAPHAEL CAVALCANTI RIBEIRO

DESENVOLVIMENTO DE UMA API DE AUTENTICAÇÃO MULTIBIOMÉTRICA

JOÃO PESSOA – PB

2018

JOÃO RAPHAEL CAVALCANTI RIBEIRO

DESENVOLVIMENTO DE UMA API DE AUTENTICAÇÃO MULTIBIOMÉTRICA

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação do Centro Universitário de João Pessoa - UNIPÊ, como pré-requisito para a obtenção do grau de Bacharel em Ciência da Computação, sob orientação do Prof. Ms. Fábio Falcão de França.

JOÃO PESSOA - PB

2018

R484d Ribeiro, João Raphael Cavalcanti.
Desenvolvimento de uma API de Autenticação Multibiométrica / João Raphael Cavalcanti Ribeiro. - João Pessoa, 2018.
52f.

Orientador (a): Prof. Ms. Fábio Falcão de França.
Monografia (Curso de Ciência da Computação) – Centro Universitário de João Pessoa – UNIPÊ.

1. Biometria. 2. Multibiometria. 3. Reconhecimento Biométrico. 4. Autenticação. 5. Impressão Digital. 6. Reconhecimento Facial. I. Titulo

UNIPÊ / BC CDU – 343.982.34

JOÃO RAPHAEL CAVALCANTI RIBEIRO

DESENVOLVIMENTO DE UMA API DE AUTENTICAÇÃO MULTIBIOMÉTRICA

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação do Centro Universitário de João Pessoa - UNIPÊ, como pré-requisito para a obtenção do grau de Bacharel em Ciência da Computação, apreciada pela Banca Examinadora composta pelos seguintes membros:

Aprovada em _____/_____/2018.

BANCA EXAMINADORA

_____

Prof. Ms. Fábio Falcão de França (UNIPÊ)

_____

Prof. Ms. Ricardo Roberto de Lima (UNIPÊ)

_____

Prof. Ms. Hilário Tomaz de Oliveira (UNIPÊ)

Dedico este trabalho a Deus que me guia pelo caminho do bem e a minha família pelo esforço para a minha formação.

Muito obrigado.

AGRADECIMENTOS

Agradeço a Deus por me permitir chegar onde estou, por me proteger e dar sabedoria para que eu trilhe o meu caminho.

Aos meus pais Antônio e Eliete e as minhas irmãs Anna e Alessandra, pelo incentivo a mim dedicados, foram eles que estiveram ao meu lado nos momentos difíceis desta jornada e me apoiaram para que eu continuasse em frente e concluísse este trabalho.

Aos meus amigos pela amizade e companheirismo durante esses anos, pelas experiências adquiridas em conjunto e esforço para obtermos mais conhecimento e pelos grupos de estudos. Muito obrigado!

Ao professor Fábio Falcão, pela dedicação, atenção e paciência, pelos ensinamentos e conhecimentos repartidos e pelo vínculo de amizade criado.

RESUMO

O presente trabalho de conclusão de curso tematiza o reconhecimento biométrico, tendo em vista o uso para a autenticação de indivíduos. O uso da biometria para a autenticação de indivíduos vem aumentando com o passar do tempo e está cada vez mais presente no nosso dia a dia. Essa técnica apresenta algumas falhas que podem ser superadas pelo uso da multibiometria, que é a combinação de mais de uma característica biométrica. Neste trabalho são coletadas as informações sobre técnicas de reconhecimento biométrico, fazendo a comparação para definir as técnicas que serão utilizadas no desenvolvimento do trabalho. Este trabalho apresenta o estudo de algumas técnicas de reconhecimento biométrico, as características utilizadas, realização da captura e o nível de maturidade. Será apresentado também o desenvolvimento de uma API de autenticação multibiométrica que utiliza impressão digital e reconhecimento facial, permitindo que aplicações utilizem esse serviço para autenticar os indivíduos, bem como a modelagem de uma arquitetura de *software* e alguns artefatos que contribuíram para o desenvolvimento do trabalho.

Palavras-Chave: Biometria. Multibiometria. Reconhecimento Biométrico. Autenticação. Impressão Digital. Reconhecimento Facial.

ABSTRACT

The present work of the course conclusion thematizes the biometric recognition, considering the use for the authentication of individuals. The use of biometrics for the authentication of individuals has been increasing over time and is increasingly present in our daily lives. This technique presents some flaws that can be overcome by the use of multibiometry, which is the combination of more than one biometric characteristic. In this work the information about biometric recognition techniques is collected, making the comparison to define the techniques that will be used in the development of the work. This work presents the study of some techniques of biometric recognition, the characteristics used, the accomplishment of the capture and level of maturity. Also will be presented the development of a multibiometric authentication API that uses fingerprint and facial recognition, allowing applications to use to authenticate the individuals, as well as modeling a software architecture and some artifacts that contribute to the development of the work.

Keywords: Biometrics. Multibiometrics. Biometric Recognition. Authentication. Fingerprint. Facial Recognition.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAM – *Active Appearance Model*

API – *Application Programming Interface*

ANSI – *American National Standards Institute*

CCD – *Charge-Coupled Device*

DER – Diagrama Entidade-Relacionamento

FAR – *False Accept Rate*

FBG – *Face Bunch Graphs*

FRR – *False Reject Rate*

ICA – *Independent Component Analysis*

IEC – *International Electrotechnical Commision*

ISO – *International Standardization Organization*

LBP – *Local Binary Patterns*

LDA – *Linear Discriminant Analysis*

OTP – *One-Time Password*

PCA – *Principal Component Analysis*

PIN – *Personal Identification Number*

PIP – *Python Index Package*

SGBDOR – Sistema de Gerenciamento de Banco de Dados Objeto Relacional

SGSI – Sistema de Gestão de Segurança da Informação

SIFT – *Scale Invariant Feature Transformation*

SI – Segurança da Informação

SO – Sistema Operacional

SQL – *Structured Query Language*

UML – *Unified Modeling Language*

SUMÁRIO

1 INTRODUÇÃO

A biometria é uma área de estudo que utiliza análise estatística e quantitativa com o objetivo de identificar características do corpo humano que são únicas para cada ser humano. Nos últimos anos, essa área está sendo relacionada ao reconhecimento biométrico, que é a geração de dados através da identificação das medidas e estruturas de órgãos, passíveis de diferenciar pessoas (MORAES, 2010).

Os Sistemas Biométricos são soluções que utilizam a biometria para a identificação de indivíduos. Esses sistemas são considerados os mais seguros para identificação, pois através de dispositivos que permitam a captura de informações biométricas, é possível verificar características fisiológicas e/ou comportamentais presentes unicamente em cada pessoa.

Através do reconhecimento biométrico, a Segurança da Informação (SI) pode coletar e utilizar os dados gerados, com o objetivo de verificar se esses dados, referentes a um determinado indivíduo, permite ou não o acesso dele a determinadas informações. O reconhecimento biométrico geralmente é utilizado para validar o acesso a um determinado sistema, mas nada impede de ser utilizado para outros fins.

Atualmente esses sistemas estão cada vez mais presentes no dia a dia das pessoas, sejam em agências bancárias, aeroportos, urnas eletrônicas, como também em outros locais de trabalho. Isso ocorre devido a sua utilização tornar a identificação e verificação de indivíduos mais segura e confiável, por seguir requisitos como Universalidade, Singularidade e Permanência das características biométricas em cada pessoa (GALVÃO, 2015; GOODRICH; TAMASSIA, 2013).

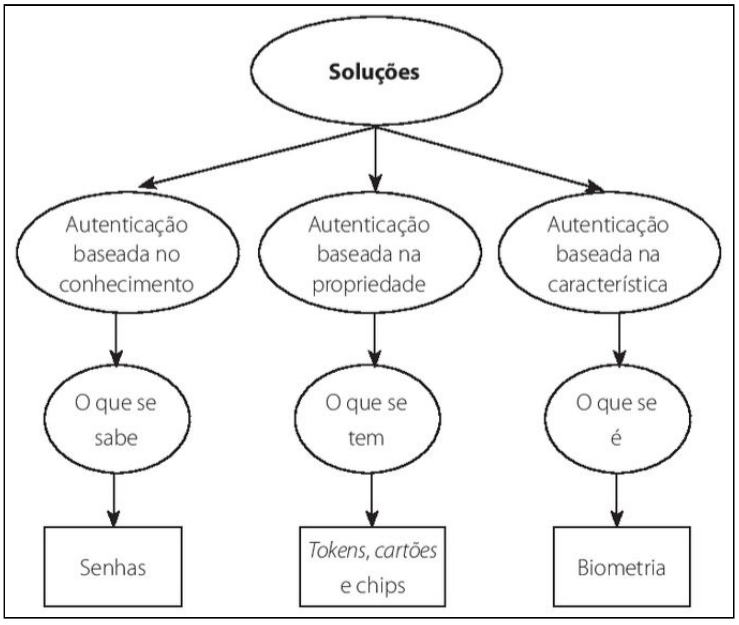
Porém, qual a importância de se utilizar reconhecimento biométrico para autenticação dos indivíduos? Quais as principais categorias de reconhecimento biométrico? Quais as melhores categorias de reconhecimento biométrico com relação ao custo benefício?

O propósito desse trabalho tem como cerne, a pesquisa das principais técnicas de reconhecimento biométrico e escolha dentre estas, aquelas que sejam de melhor custo/benefício para implantação em aplicações *web*, a fim de que seja possível desenvolver uma interface de aplicação (API) que utilize a multibiometria para autenticação de indivíduos.

1.1 RELEVÂNCIA DO ESTUDO

Conforme o avanço tecnológico e o grande número de dados trafegados pela internet nos dias de hoje, a segurança da informação passou a ser um pilar fundamental para que esses dados fiquem protegidos impedindo que sejam acessados por pessoas que não tenham essa autorização (BEAL, 2008; FONTES, 2006). Com isso um dos pilares que os sistemas de controle de acesso atingem é a confidencialidade, e será abordado especificamente este pilar, através de técnicas biométricas.

Figura 1 – Tipos de Autenticação



Fonte: Adaptado de Galvão (2015, p. 32).

De acordo com a Figura 1, os sistemas computacionais podem utilizar três processos de autenticação, baseado em conhecimento, propriedade ou características. É comum os sistemas utilizarem autenticação baseada em conhecimento através da utilização de senhas. Esse processo pode apresentar algumas vulnerabilidades como esquecimento, roubo ou descoberta da senha, possibilitando acesso indevido de uma pessoa não-autorizada. Já os sistemas que utilizam autenticação baseada em propriedade, utilizam um dispositivo criptográfico que possuem informações para autenticação, além de ser utilizado em conjunto com uma senha. Podem apresentar vulnerabilidades como perda ou roubo do dispositivo, o que impede a utilização para autenticação, mas um indivíduo apenas com a posse do dispositivo não conseguirá se autenticar no sistema. Por fim, existem os sistemas que utilizam autenticação baseada em características (biometria), esse processo apresenta algumas vantagens em relação aos processos anteriores, pois o indivíduo não precisa carregar nenhum dispositivo nem lembrar de senhas para realizar a autenticação em um sistema, além de que uma característica biométrica não pode ser roubada ou emprestada (GALVÃO, 2015; MORAES, 2010).

Na maioria desses sistemas está presente apenas uma técnica de reconhecimento biométrico (monobiométrico), para aumentar a precisão nas verificações dos indivíduos nesses sistemas é possível combinar várias técnicas (multibiometria), minimizando problemas importantes como ruídos e ataques de impostores (HONG; JAIN; PANKANTI, 1999; ROSS; NANDAKUMAR; JAIN, 2006).

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Desenvolver uma API de autenticação que utilize reconhecimento multibiométrico nas verificações dos indivíduos durante o controle de acesso à sistemas computacionais, com foco em aplicações *web*.

1.2.2 Objetivos Específicos

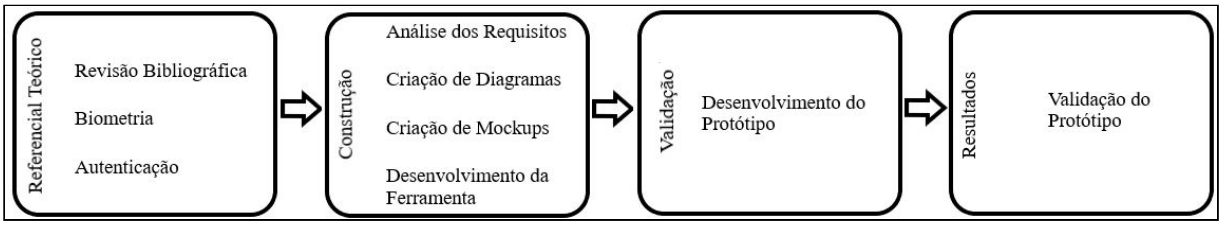
- Analisar as técnicas de reconhecimento biométrico;

- Definir as técnicas de reconhecimento que serão utilizados no trabalho;
- Propor uma API de autenticação baseada em multibiometria;
- Implementar um protótipo para validar a API proposta.

1.3 INDICAÇÃO DA METODOLOGIA

O processo de construção deste trabalho será utilizando a metodologia estudo de caso, que consiste no estudo profundo e exaustivo de um ou poucos objetos de maneira que permita o seu amplo e detalhado conhecimento (GIL, 2002).

Figura 2 – Processo de Construção do Trabalho



Fonte: Elaborada pelo autor (2018).

Como podemos observar na Figura 2, o processo de construção deste trabalho foi dividido em etapas e será descrito a seguir. Inicia-se com a revisão bibliográfica, em que foram realizadas pesquisas para levantamento de categorias de características biométricas que poderiam ser utilizadas na construção do trabalho.

Após definir as categorias de reconhecimento biométrico que serão utilizadas no trabalho, serão realizados testes, separadamente com cada técnica, utilizando APIs que permitem a captura e/ou tratamento dos dados biométricos. Permitindo a geração de *templates* [1] biométricos para que seja possível armazenar as informações na base de dados.

Em seguida, foi modelada uma arquitetura de *software* para o desenvolvimento da API que permite a autenticação através de multibiometria, com foco em permitir a inclusão de novas técnicas de reconhecimento biométrico futuramente, sendo implementado utilizando a linguagem de programação Java. Além disso, foi implementado um protótipo na linguagem

[1] São estruturas que contém os dados referentes a biometria de um indivíduo.

Java para a plataforma *web*, utilizando o Sistema Gerenciador de Banco de Dados (SGBD) PostgreSQL.

1.4 ORGANIZAÇÃO DO TRABALHO

Após esse capítulo introdutório, o conteúdo deste trabalho organiza-se da seguinte forma:

- 2 AUTENTICAÇÃO E BIOMETRIA: apresentará os conceitos e as pesquisas que fundamentam a realização deste trabalho;
- 3 DESENVOLVIMENTO DA SOLUÇÃO: apresentará a ferramenta proposta, assim como arquitetura de *software*, diagramas, mockups de telas e demais artefatos que contribuíram com o trabalho;
- 4 CONSIDERAÇÕES FINAIS: apresentará de forma conclusiva, respostas aos objetivos específicos propostos pelo trabalho, apresentando também limitações desta pesquisa e trabalhos futuros.

2 AUTENTICAÇÃO E BIOMETRIA

Este capítulo é responsável por apresentar o embasamento teórico, expondo os conceitos e teorias, fundamentais nas áreas abordadas pelo trabalho proposto. Serão abordados conceitos sobre Segurança da Informação (SI), identificação e autenticação de indivíduos, utilização de sistemas biométricos, bem como algumas técnicas de reconhecimento biométrico. Além de descrever as APIs e ferramentas utilizadas durante o desenvolvimento desse trabalho.

Para o entendimento do trabalho é importante que se entenda o conceito de Segurança da Informação (SI). Fontes (2006, p. 11) descreve que segurança da informação é "o conjunto de orientações, normas, procedimentos, política e demais ações que tem por objetivo proteger o recurso informação". Já Beal (2008, p. 01) descreve como "o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade". Sendo assim, poderemos concluir que a segurança da informação visa a proteção das informações, preservando o acesso contra pessoas não autorizadas, garantindo a disponibilidade quando necessária, a originalidade e que não sofreu modificações por indivíduos não autorizados.

A Organização Internacional para Padronização (*International Standardization Organization* ou ISO) e a Comissão Eletrotécnica Internacional (*International Electrotechnical Commision* ou IEC) são responsáveis por gerir normas internacionais referentes a diversas áreas do conhecimento. Esses órgãos formularam a norma ISO/IEC 27001 que é a norma internacional de gestão de segurança da informação. De acordo com a ISO[2], "a norma ISO/IEC 27001:2013 tem como objetivo estabelecer, implementar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)".

Conforme descrito por Beal (2008), Fontes (2006) e Moraes (2010), os principais atributos da SI são: confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade e conformidade.

- Confidencialidade é a propriedade que permite o acesso a informação apenas pelos indivíduos autorizados;
- Integridade garante que a informação se mantem original a estabelecida pelo proprietário da mesma;

[2] Disponível em: <https://www.iso.org/standard/54534.html>. Acesso em: 14/04/2017.

- Disponibilidade permite que a informação esteja sempre disponível para os usuários autorizados;
- Autenticidade garante que a informação é oriunda de um usuário declarado e que não foi modificada por indivíduos que não tenham autorização;
- Irretratabilidade ou Não Repúdio é a propriedade responsável por impossibilitar a negação da autoria de uma informação;
- Conformidade é responsável por garantir que um sistema siga as leis e regulamentações relacionados com a SI.

2.1 AUTENTICAÇÃO

"A autenticação tem por objetivo garantir que o usuário descrito na identificação é verdadeiramente essa pessoa. Isto é, busca provar que você é você. " (FONTES, 2006, p. 23). A autenticação é o ato de verificar se uma pessoa é realmente quem diz ser, ou seja, certificar a identidade de uma pessoa. Portanto, a autenticação é utilizada como uma forma de confirmar ou negar a identidade de um indivíduo, essa identidade pode ser verificada tanto no mundo real, como também no mundo digital.

Atualmente, existem vários métodos de autenticação, Fontes (2006, p. 23) descreve da seguinte forma "no ambiente computacional, você é autenticado por alguma informação que você sabe (senha), possui (cartão, *token*[3]) ou é (características física-biometria) ". Esses métodos se baseiam no que o indivíduo sabe (conhecimento), possui (propriedade) ou nas características do indivíduo (característica). Também existe a possibilidade de combinar esses métodos com o intuito de aumentar o nível de segurança. As combinações desses métodos tornam a autenticação de um indivíduo mais segura, pois exigem algo que ele saiba, tenha ou seja (GALVÃO, 2015; MORAES, 2010; NAKAMURA; GEUS, 2007). Como por exemplo, combinar o uso de *token* e senha, reconhecimento facial e senha, cartão e impressão digital ou até mesmo mais de uma característica biométrica (multibiometria), como impressão digital e reconhecimento facial. Alguns exemplos de técnicas de reconhecimento biométrico são: Impressão Digital, Retina, Reconhecimento Facial, Íris, Geometria das Mãos, Reconhecimento de Voz e Reconhecimento de Assinatura.

[3] Dispositivo eletrônico de armazenamento e/ou geração de senhas.

Todos os métodos possuem pontos positivos e negativos, a utilização deles será de acordo com o grau de segurança ao acesso. A combinação de dois métodos de autenticação é chamada de autenticação em dois fatores e quando se utilizam três deles é chamada de autenticação em três fatores (NAKAMURA; GEUS, 2007). Esses métodos serão descritos a seguir.

2.1.1 Autenticação baseada no Conhecimento

É fundamentada em algum conhecimento do usuário, ou seja, baseia-se em algo que o usuário saiba. O meio mais utilizado são as senhas, mas existem outros meios como por exemplo: chave criptográfica, *Personal Identification Number* (PIN) e identificação positiva, que são informações pessoais fornecidas pelo usuário para que sejam validadas pelo sistema de autenticação, essas informações são de conhecimento do sistema desde o cadastro do usuário. A identificação positiva é mais comum de ser usada pelas instituições bancárias para validar transações (NAKAMURA; GEUS, 2007).

Para aumentar a segurança e força da senha é aconselhável implementar políticas para definição de senhas, como exigir que as senhas contenham caracteres alfanuméricos e especiais, não permitir a utilização das últimas cinco senhas cadastradas anteriormente, definir uma quantidade mínima de caracteres e/ou definir um intervalo de tempo para mudança da senha (MORAES, 2010).

A principal vantagem é que os usuários já estão familiarizados com a utilização desse método. Já as principais desvantagens são o esquecimento, a utilização de senhas fracas, uso de senhas com informações pessoais de conhecimento compartilhado (data de nascimento, cidade natal, nome do time de futebol), acesso a arquivos de senhas do usuário e monitoramento e captura de senhas (FONTES, 2006; MORAES, 2010).

2.1.2 Autenticação baseada na Propriedade

Fundamenta-se em algum dispositivo que o usuário possui e pode ser dividido em dispositivos de memória e dispositivos inteligentes. Os dispositivos de memória são responsáveis apenas por armazenar as informações e muitas vezes são combinados com as senhas. Um exemplo desse tipo de dispositivo são os cartões bancários magnéticos, que

apenas armazenam as informações sem realizar o processamento delas. Já os dispositivos inteligentes possuem circuitos para o processamento de algumas informações que serão armazenadas (MORAES, 2010; NAKAMURA; GEUS, 2007).

Figura 3 – eToken 5110 (*Token*)

Fonte: Gemalto[4].

Alguns exemplos desses tipos de dispositivos são os *tokens* (ver Figura 3), eles geralmente são dispositivos que se conectam através de portas de comunicação USB e realizam o processamento das informações ao serem utilizadas.

Figura 4 – eToken PASS OTP Authenticator (*Token* OTP)

Fonte: Gemalto[5].

Já os *tokens* OTP (*One-Time Password*) (ver Figura 4), fazem parte de outra categoria de *token* que geram senhas dinâmicas baseado em um tempo definido (geralmente 30 ou 60 segundos), dessa forma só será possível utilizar a senha gerada dentro do tempo limite. Por

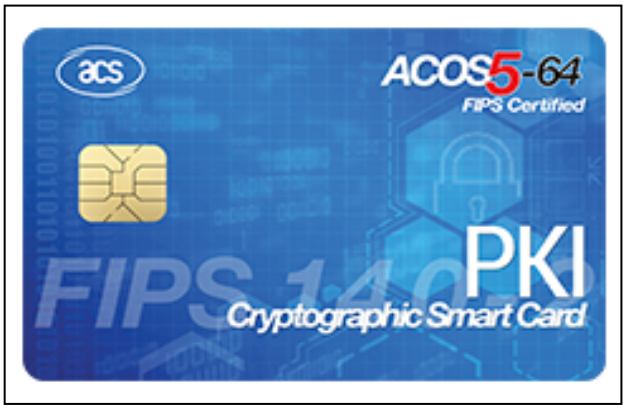
[4] Disponível em: <https://safenet.gemalto.com/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-5110-usb-token/>. Acesso em: 31/03/2018.

[5] Disponível em: <https://safenet.gemalto.com/multi-factor-authentication/authenticators/one-time-password-otp/>. Acesso em: 26/04/2017.

gerarem senhas, esses dispositivos possuem um pequeno visor LCD, bateria e um botão para geração de senhas dinâmicas.

E os cartões inteligentes (*smart cards*) que possuem circuitos elétricos para realizar o processamento e armazenamento das informações (ver Figura 5). São do tamanho de um cartão de crédito magnético, mas possuem CPU, memória e chip criptográfico incorporados, além de possuir proteção por senha.

Figura 5 – ACOS5-64 V3.00 Cryptographic Card (*Smart Card*)



Fonte: Advanced Card Systems Holdings Limited[6].

O principal ponto positivo é que resolve os problemas com as senhas comuns, mas as desvantagens são o alto custo em comparação com o método anterior, pois é preciso um *hardware* específico, e a possibilidade de perda ou roubo do dispositivo gerando oportunidade de acesso não-autorizado (GALVÃO, 2015; NAKAMURA; GEUS, 2007).

2.1.3 Autenticação baseada na Característica

É baseada em alguma característica física ou comportamental do indivíduo e é comumente conhecida como Biometria. Esse método de autenticação é considerado mais seguro do que os anteriores, pois aumenta a dificuldade de um indivíduo autenticar-se no sistema se passando por outra pessoa e foi proposto devido aos problemas encontrados nos métodos descritos anteriormente. Essa autenticação evita os problemas de esquecimento e perda dos dispositivos, que são algumas desvantagens presentes nos outros métodos. Alguns

[6] Disponível em: <http://www.acs.com.hk/en/products/308/acos5-64-cryptographic-card-contact>. Acesso em: 26/04/2017.

exemplos desse tipo de autenticação são o reconhecimento de características faciais, impressão digital e reconhecimento da íris do olho (MORAES, 2010; NAKAMURA; GEUS, 2007).

As principais vantagens são o aumento do nível de segurança tendo em vista tratar-se de características estatisticamente únicas, não existirá o esquecimento das informações, bem como a perda do dispositivo necessários para a autenticação. As principais desvantagens são o custo elevado de alguns sensores responsáveis pela captura das informações, o ruído na captura que podem dificultar o reconhecimento e a intrusividade na captura dos dados biométricos que é o contato do sensor com o indivíduo (JAIN; ROSS; NANDAKUMAR, 2011; NAKAMURA; GEUS, 2007).

2.2 BIOMETRIA

A biometria é a ciência que se utiliza da aplicação de métodos estatísticos e quantitativos sobre características físicas, biológicas ou comportamentais de um indivíduo para que seja possível reconhecer ou verificar a sua identidade. Ela é considerada como um tipo de autenticação mais segura com relação às demais, pois utiliza-se de um método de reconhecimento através de aspectos humanos intrínsecos, ou seja, cada indivíduo possui características estatisticamente únicas, tanto no âmbito Fisiológico como no Comportamental, apesar de ainda existirem alguns problemas. Portanto, com a utilização desse método torna-se mais difícil a falsificação da identidade de um indivíduo (NAKAMURA; GEUS, 2007).

A biometria utiliza-se de sistemas de reconhecimento para processar as informações referentes as características que serão reconhecidas. Esses sistemas irão identificar, armazenar e aplicar algoritmos para medir pontos específicos de cada tipo de característica, para que seja possível validar a utilização destas informações. O reconhecimento é feito através de sensores específicos para a identificação biométrica, variando de tamanho e preço de acordo com o tipo de técnica. Existem também sistemas que utilizam mais de uma característica biométrica para autenticar a identidade de um indivíduo e são chamados de sistemas multibiométricos. Esses sistemas podem ser considerados mais seguros do que os que possuem apenas um tipo de reconhecimento, pois o sistema terá mais informações de características únicas do indivíduo

obtendo maior precisão para autenticar a sua identidade (NAKAMURA; GEUS, 2007; ZHANG; GUO; GONG, 2015).

Existem vários tipos de características biométricas que podem ser utilizadas no processo de reconhecimento de um indivíduo. A seguir, serão apresentadas as categorias de impressão digital, reconhecimento facial e reconhecimento de íris.

2.2.1 Impressão Digital

O reconhecimento de impressões digitais é a categoria mais utilizada e que é empregado na maioria das aplicações. Esse reconhecimento utiliza sensores eletrônicos chamados leitores biométricos, que funcionam principalmente através de tecnologia óptica ou capacitiva. Os sensores que funcionam através da tecnologia óptica utilizam uma placa de vidro, uma fonte de luz com tecnologia LED[7] e uma câmera com dispositivo de carga acoplada (CCD)[8] para a construção das imagens de impressões digitais. Quando um dedo é colocado sobre a placa de vidro, a fonte de luz ilumina o vidro com um certo ângulo e a câmera é colocada em uma posição que possa capturar a luz refletida do vidro. A luz incidente sobre as cristas é aleatoriamente dispersa e resulta em uma imagem escura, enquanto a luz incidente sobre os vales sofre reflexão interna e resulta em uma imagem brilhante. Através dessas imagens é construída uma imagem referente a impressão digital. Já os sensores que funcionam através da tecnologia capacitiva utilizam um conjunto de eletrodos em milhares de pequenas placas de capacitância incorporados em um chip. Esses sensores possuem tamanho muito pequeno e podem ser facilmente incorporados em *notebooks* e *smartphones*. A pele da impressão digital funciona como outro eletrodo ao entrar em contado com o sensor, formando um condensador em miniatura. Sendo assim, as cristas e vales das impressões digitais resultam em capacitância diferente, essa diferença é a base para o mapeamento e captura das digitais do indivíduo. (JAIN; ROSS; NANDAKUMAR, 2011; PEREIRA, 2013; RATHA; SENIOR; BOLLE, 2001).

Os sensores e sistemas de reconhecimento de impressão digital capturam o padrão único das linhas do dedo, esse padrão dá-se o nome de minúcias. Essas linhas se formam durante o quarto mês de gestação do bebê e permanecem nos dedos durante toda a vida. A

[7] Dispositivo eletrônico semicondutor e emissor de luz (YOUNG; FREEDMAN, 2009).
[8] Dispositivo eletrônico semicondutor para captação de imagens (YOUNG; FREEDMAN, 2009).

identificação de um indivíduo pode ser feita quando se encontram no mínimo 12 características idênticas na impressão digital (MORAES, 2010).

Figura 6 – Imagem de uma impressão digital

Fonte: Adaptado de Jain; Ross e Nandakumar (2011, p. 53).

Na Figura 6, podemos observar a impressão digital de um dedo, que possuem várias linhas chamadas de minúcias. As minúcias são pontos específicos nas pequenas linhas presentes nas impressões digitais. Essas linhas possuem grande importância, pois os reconhecimentos digitais utilizam elas para que seja possível reconhecer um indivíduo. As minúcias possuem vários formatos, dentre eles crista final ou terminação, crista bifurcada, inclusão e ilha. A crista terminação é caracterizada pelo ponto onde a linha termina. Já a crista bifurcada caracteriza-se pelo ponto onde a linha se divide, causando uma ramificação. A crista inclusão é caracterizada pelo ponto onde a linha se divide e une imediatamente, causando um pequeno espaço circular ou elíptico. E por fim, a crista ilha que é caracterizada por uma pequena linha que forma uma ilha (GALTON, 1892; JAIN; ROSS; NANDAKUMAR, 2011; ZHANG; GUO; GONG, 2015).

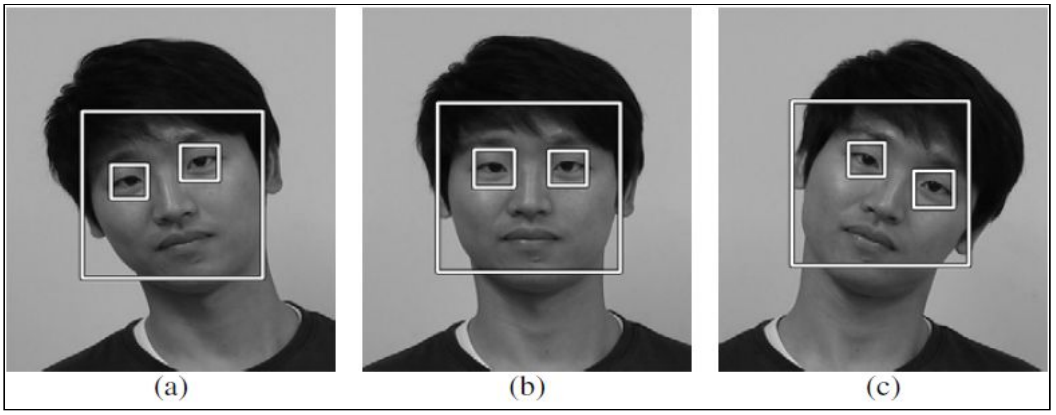
Por ser uma das categorias mais utilizadas, é evidente que possua um alto nível de maturidade, decorrente de muitos anos de pesquisas. Portanto, é natural que indivíduos mal-intencionados tentem burlar esse sistema, buscando de forma indevida a autenticação da identidade de outro indivíduo. Com a preocupação em manter esse reconhecimento seguro e diminuir as taxas de falsa aceitação, foram desenvolvidas técnicas para detecção de impressões digitais falsas tanto a nível de *software* quanto a nível de *hardware* (PEREIRA, 2013).

2.2.2 Reconhecimento Facial

O reconhecimento facial utiliza-se da imagem da face de um indivíduo para realizar as medições das características do rosto. Esse reconhecimento é feito através da aplicação de algoritmos para a detecção de uma face que é obtida por meio de uma imagem ou vídeo. Após essa detecção, são aplicados outros algoritmos para medir, identificar e comparar características da face e assim gerar dados que possam ser utilizados para a autenticação do indivíduo (JAIN; LI, 2011; JAIN; ROSS; NANDAKUMAR, 2011).

Existem diversos algoritmos para detecção facial, mas o mais conhecido é o Algoritmo de Viola-Jones. Esse algoritmo foi desenvolvido com o objetivo de detectar objetos em uma imagem, ele pode ser utilizado para reconhecer qualquer objeto, mas é frequentemente utilizado para a detecção facial e o ponto forte é a rapidez com que é executado. Na Figura 7 podemos observar um exemplo de detecção de face utilizando o algoritmo Viola-Jones. Outros algoritmos existentes utilizam variações das ideias presentes neste algoritmo (BRAGA, 2013).

Figura 7 – Exemplo de detecção de face e olhos usando o algoritmo Viola-Jones



Fonte: Jain; Ross e Nandakumar (2011, p. 117).

Existem três principais tipos de métodos para medição e identificação de características faciais, eles podem ser baseados em aparência, em modelos e em textura, e serão descritos abaixo (JAIN; ROSS; NANDAKUMAR, 2011).

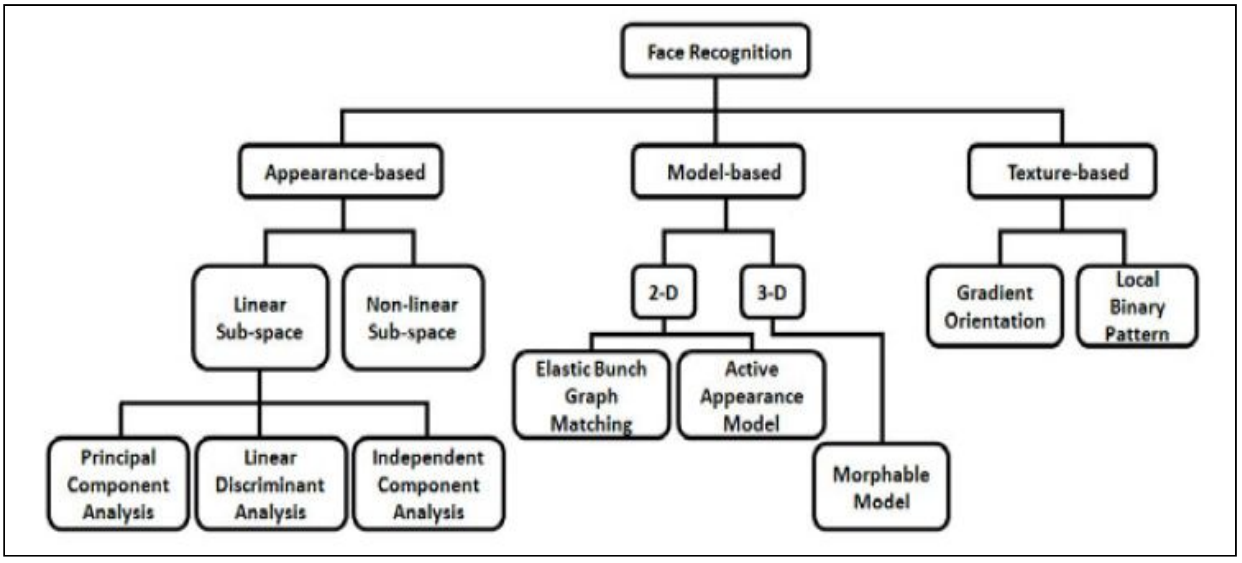
- Os métodos baseados em aparência geram uma representação compacta da face através da imagem capturada, mapeando a imagem da face. O mapeamento pode ser linear ou não linear, os principais algoritmos utilizam projeções lineares como Análise

de Componentes Principais (*Principal Component Analysis* ou PCA), Análise Discriminante Linear (*Linear Discriminant Analysis* ou LDA) e Análise de Componentes Independentes (*Independent Component Analysis* ou ICA);

- Os métodos baseados em modelo tentam construir modelos de face 2D ou 3D com o intuito de facilitar a correspondência de imagens de face a partir de variações de pose, esse método requer a detecção de vários pontos da face como os olhos, nariz e boca. Os principais algoritmos de modelos de face 2D são *Face Bunch Graphs* (FBG) e *Active Appearance Model* (AAM) e o principal algoritmo de modelos de face 3D é o *Morphable Model*;
- Os métodos baseados em textura tentam encontrar características que sejam invariantes de pose e iluminação. Alguns exemplos de características são orientação gradiente, *Local Binary Patterns* (LBP) e *Scale Invariant Feature Transformation* (SIFT).

Na Figura 8 é apresentado as principais categorias de reconhecimento facial, bem como as técnicas utilizadas, citando alguns algoritmos que implementam os conceitos básicos provenientes dessas técnicas.

Figura 8 – Categorização das técnicas de reconhecimento facial.



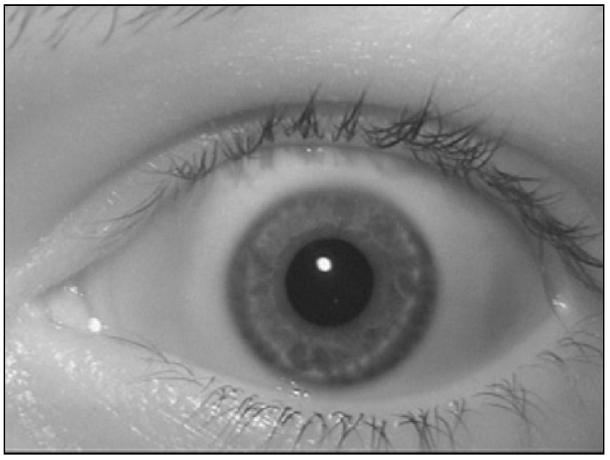
Fonte: Jain; Ross e Nandakumar (2011, p. 117).

Essa categoria possui baixo custo de implementação com relação aos equipamentos, pois não são necessários sensores sofisticados para a captura das imagens e vídeos. A técnica de reconhecimento é não intrusiva e possui um nível médio de maturidade (RATHA; SENIOR; BOLLE, 2001).

2.2.3 Reconhecimento de Íris

A íris é um órgão interno do olho que se localiza atrás da córnea e na frente do cristalino. É responsável por controlar a quantidade de luz que entra no olho, dilatando ou contraindo uma pequena abertura chamada pupila (JAIN; ROSS; NANDAKUMAR, 2011; NEHEMY, 2015). Ela é conhecida como a parte colorida do olho, delimitada pelas pupila e esclera (parte branca do olho), e é extremamente rica em textura (RATHA; SENIOR; BOLLE, 2001). A Figura 9 mostra a imagem do olho humano capturada por meio da tecnologia infravermelha, no centro do olho encontra-se uma parte mais escura que é a pupila, a parte branca é a esclera e a parte cinzenta que se encontra entre a pupila e a esclera é a íris. A estrutura da íris é definida por volta de um ano de idade e permanece constante. Existem diferenças entre a íris dos olhos de gêmeos idênticos e até entre os olhos direito e esquerdo da mesma pessoa (RAKESH; KHOGARE, 2012).

Figura 9 – Imagem do olho humano



Fonte: Jain; Ross e Nandakumar (2011, p. 164).

Um típico sistema de reconhecimento de íris é dividido em quatro módulos: aquisição, segmentação, normalização e codificação/comparação. O módulo de aquisição é responsável pela captura da imagem do olho humano através de sensores que utilizam tecnologia infravermelha, para a detecção da íris e captura da imagem. O módulo de segmentação é responsável por localizar e detectar os limites internos e externos da íris na imagem do olho. O módulo de normalização é caracterizado por aplicar algoritmos geométricos para transformar a imagem da íris da forma circular para a forma retangular, para facilitar a codificação das suas características. O módulo de codificação/comparação é responsável por extrair as características da textura da íris, para que sejam utilizadas na geração de um código, para que possibilite o armazenamento e/ou a comparação futuramente (JAIN; ROSS; NANDAKUMAR, 2011; RAKESH; KHOGARE, 2012).

2.3 TECNOLOGIAS UTILIZADAS

Para o desenvolvimento do trabalho será utilizado a linguagem de programação JAVA, que é uma linguagem de programação interpretada, orientada a objetos e portável, ou seja, pode ser executado em diferentes arquiteturas e sistemas operacionais (DEITEL, H.; DEITEL, P., 2005).

Com relação a base de dados, será utilizado o PostgreSQL, que é um Sistema de Gerenciamento de Banco de Dados Objeto Relacional (SGBDOR), possui código fonte aberto, suporta grande parte do padrão SQL (*Structured Query Language*), além de diversos outros recursos (POSTGRESQL, 2017).

Os dados biométricos das impressões digitais seguem a padronização de acordo com a *American National Standards Institute* (ANSI) que definiu a norma ANSI 381 especificando um formato para a troca de dados de reconhecimento de impressões digitais baseadas em imagens, definindo o conteúdo, o formato e as unidades de medidas para essas informações (ANSI, 2017). Após a captura das minúcias da impressão digital, será gerado um *template* no formato especificado por essa norma.

Com o objetivo de padronizar a manipulação dos dados biométricos, a fim de permitir a serialização para o armazenamento, foi definido que eles serão tratados como *array* de *bytes*. Para a persistência na base de dados, será utilizado o tipo de dado *bytea* que no

PostgreSQL é um tipo de dado que permite o armazenamento de cadeias binárias, ou seja, uma sequência de *bytes* (POSTGRESQL, 2017).

Para a criação de diagramas, foi utilizado a ferramenta *Astah*[9], na versão *Community*, que permite a criação de diagramas UML. Esta ferramenta possibilitou a criação dos diagramas de classe, de componentes e atividades. Já para a modelagem da base de dados, foi utilizado a ferramenta *MySQL Workbench*[10], que permite a criação de tabelas relacionais e geração de Diagramas Entidade-Relacionamento (DER).

Abaixo serão descritos com mais detalhes algumas tecnologias que foram utilizadas no desenvolvimento deste trabalho e que impactaram diretamente na implementação da API proposta.

2.3.1 Spring Framework

O *Spring Framework*[11] é um *framework*[12] *open source*[13] desenvolvido utilizando a linguagem de programação Java e se baseia nos padrões de projetos Inversão de Controle (IoC) e Injeção de Dependências (DI). É modular, o que permite utilizar apenas os projetos necessários, incluindo apenas as dependências que serão utilizadas, além de possuir vários projetos com diversas implementações que facilitam e agilizam o desenvolvimento de um aplicativo ao utilizar esse *framework*.

Dentre os principais projetos mantidos pelo *Spring* estão: *Spring Boot*, *Spring Data* e *Spring Security*. O *Spring Boot* inclui implementações e dependências que facilitam o funcionamento rápido de um projeto. Já o *Spring Data* fornece implementações que possibilitam acesso a dados armazenados em bancos de dados, disponibilizando subprojetos específicos para cada banco de dados suportado, suportando armazenamento em bancos que utilizam SQL ou NoSQL. E o *Spring Security* que fornece implementações para tornar a aplicação protegida, facilitando a implementação de autenticação e controle de acesso de usuários na aplicação.

---

[9] Disponível em: <http://astah.net/editions/community>. Acesso em: 30/03/2018.
[10] Disponível em: <https://www.mysql.com/products/workbench/>. Acesso em: 30/03/2018.
[11] Disponível em: <https://spring.io/>. Acessado em: 17/05/2018.
[12] É uma abstração de códigos comuns presentes em vários projetos de *softwares*, provendo funcionalidades genéricas.
[13] Modelo de desenvolvimento de *software* com licenciamento livre para codificação e incrementos.

2.3.2 Digital Persona SDK

A *Digital Persona*[14] é uma empresa de segurança especializada em soluções voltadas para autenticação e controle de acesso utilizando biometria e fornecem produtos como sensores biométricos e aplicativos que utilizam esses sensores.

A *Digital Persona SDK* é um kit de ferramentas de desenvolvimento que permite a comunicação com leitores de impressão digital para capturar e processar os dados gerados, permitindo que um usuário possa se autenticar para utilizar o computador ou algum sistema que utilize autenticação através de reconhecimento de impressão digital. Este SDK fornece as bibliotecas, em diversas linguagens de programação, para construção de *softwares* que podem utilizar os leitores de impressão digital, além de fornecer a documentação descrevendo as interfaces e métodos disponibilizados, e códigos de exemplos que usam o leitor para captura e reconhecimento das impressões digitais.

2.3.3 Dlib

A Dlib[15] é uma biblioteca de código aberto (*open source*) desenvolvida utilizando a linguagem de programação C++ e que contém algoritmos e ferramentas de aprendizagem de máquina (*machine learning*), processamento de imagem, reconhecimento facial, dentre diversos outros algoritmos que auxiliam na criação de *softwares* complexos (DLIB, 2018).

Algumas das principais características dessa biblioteca são o fornecimento de documentação completa das classes e funções, exemplos de códigos para utilização e portabilidade que é a utilização da biblioteca em várias plataformas diferentes, além de *wrappers* da API que fornecem interfaces referentes ao uso dos algoritmos, permitindo a utilização através de outras linguagens de programação, como Python.

Os algoritmos de reconhecimento facial disponibilizados pela Dlib alcançaram a precisão de 99,38% de taxa de acerto no benchmark *Label Faces in the Wild*[16], que é um banco de dados de fotografias de rosto projetado para estudos sobre reconhecimento facial.

---

[14] Disponível em: <https://www.crossmatch.com/>. Acesso em: 17/05/2018.
[15] Disponível em: <http://dlib.net/>. Acesso em: 17/05/2018.
[16] Disponível em: <http://vis-www.cs.umass.edu/lfw/>. Acesso em: 23/06/2018.

Para o processamento de reconhecimento facial, a Dlib utiliza *deep learning* implementando um modelo de rede neural ResNet com 27 camadas conv, sendo uma versão modificada da rede ResNet-34 que tem como objetivo a Aprendizagem Residual Profunda para Reconhecimento de Imagem, sendo adaptado com a remoção de algumas camadas e reduzindo o número de filtros por camada pela metade[17].

2.3.4 Face Recognition API

É uma API desenvolvida através da linguagem de programação Python e que utiliza a biblioteca Dlib, tendo como objetivo prover algoritmos relacionados ao reconhecimento facial, fornecendo implementações para localização de faces em imagens, além de comparar imagens que contém faces e verificar se elas pertencem a mesma pessoa. Ela pode ser encontrada no Github[18], onde contém a implementação, documentação e códigos de exemplos.

Para a sua utilização, é necessário que seja instalado o Python 3.3+, Visual Studio 15 juntamente com o Visual C++ Compiler e a instalação da biblioteca Dlib através do PIP (*Python Index Package*), que é um sistema de gerenciamento de pacotes de *softwares* escritos na linguagem Python.

[17] Disponível em: <https://github.com/davisking/dlib-models>. Acesso em: 25/06/2018.

[18] Disponível em: <https://github.com/ageitgey/face_recognition>. Acesso em: 17/05/2018.

3 DESENVOLVIMENTO DA SOLUÇÃO

A motivação para este trabalho ocorre tendo em vista que com o surgimento de sistemas de reconhecimento biométricos, foram identificados que apesar da autenticação baseada em característica ser mais segura do que as baseadas em conhecimento ou em propriedade, esses sistemas podem apresentar alguns desafios como ruídos na captura (ex. sujeira no sensor ou cicatriz), ataques de mascaramento ou imitação (ex. tentar se passar por outro indivíduo), entre outros. Com o avanço tecnológico, surgiram os sistemas de reconhecimento multibiométrico que utilizam mais de uma característica biométrica, fazendo com que esses desafios sejam minimizados devido a fusão de informações apresentadas por múltiplas fontes (HONG; JAIN; PANKANTI, 1999; ROSS; NANDAKUMAR; JAIN, 2006).

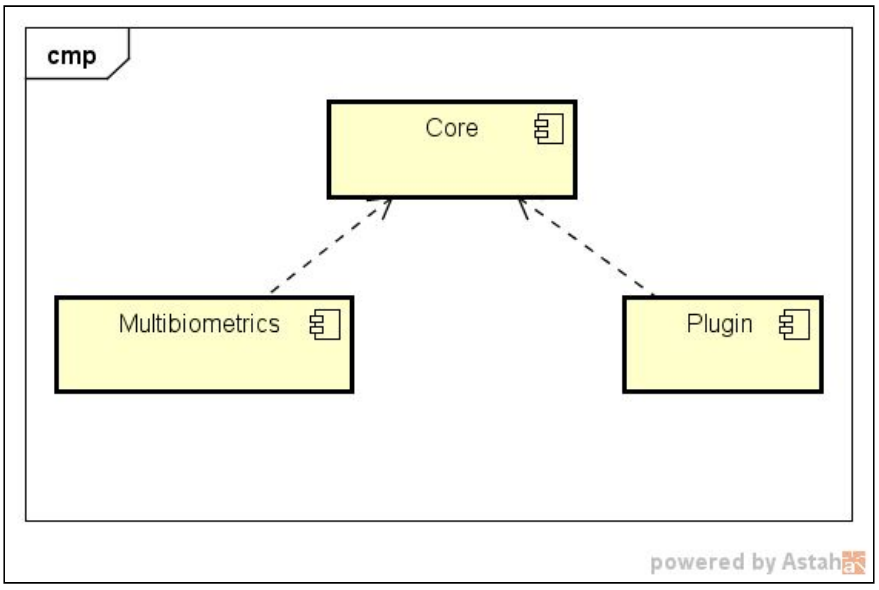
A solução que está sendo desenvolvida é uma API que disponibilizará funcionalidades para a autenticação multibiométrica de indivíduos, implementando o reconhecimento multibiométrico através do uso de impressão digital e reconhecimento facial, permitindo que apenas os indivíduos autenticados acessem um determinado sistema.

Este capítulo apresenta o desenvolvimento do trabalho, bem como a arquitetura do *software*, diagramas e demais artefatos que auxiliaram no desenvolver do trabalho.

3.1 ARQUITETURA DA SOLUÇÃO

A arquitetura visa à construção de uma API para autenticação multibiométrica de indivíduos, tendo como objetivos a possibilidade de inserir novas categorias de reconhecimento biométrico sem a necessidade de remodelar a arquitetura e permitindo configurar quais as categorias que serão utilizadas para a autenticação de cada indivíduo. De acordo com a descrição de Silva, Gomide e Petrillo (2003, p. 107), “arquitetura de *software* é uma visualização conceitual da estrutura de um aplicativo. Nela são definidos todos os componentes de *hardware* e de *software* que formam uma aplicação”.

Figura 10 – Arquitetura de Componentes da Solução



Fonte: Elaborada pelo autor (2018).

A Figura 10 ilustra o diagrama UML (*Unified Modeling Language*) de componentes da arquitetura. Os componentes são artefatos de *software* que possuem detalhes de implementação, fornecendo interfaces públicas que expõem os serviços que poderão ser utilizados. Nas subseções a seguir serão descritos os componentes da arquitetura apresentados no diagrama, bem como as relações entre cada um deles.

3.1.1 Core

O componente *Core* abrange a camada referente à regra de negócio. A regra de negócio é responsável por unir todas as regras de domínio da aplicação, tendo como cerne satisfazer os objetivos do domínio (SILVA; GOMIDE; PETRILLO, 2003). Este componente provê serviços de acesso a dados, intermediando a recuperação e armazenamento dos dados, sem que tenha conhecimento de como essas operações são realizadas. Também é responsável por possuir implementações que facilitará a comunicação e troca de informações entre os componentes *Plugin* e *Multibiometrics*.

3.1.2 Plugin

O componente *Plugin* é responsável por conter os algoritmos que possibilitam a captura dos dados biométricos dos indivíduos e executa um serviço, na máquina do cliente, para que seja possível capturar esses dados através dos sensores e enviá-los para a aplicação no servidor. Este serviço se comunicará diretamente com os drivers dos sensores, possibilitando a sua utilização na máquina dos usuários.

3.1.3 Multibiometrics

O componente *Multibiometrics* é responsável por prover um conjunto de algoritmos que permita o controle de acesso, utilizando autenticação multibiométrica, em que os indivíduos possam fornecer os dados necessários primeiramente para o cadastro e posteriormente para sua identificação e autenticação.

Este componente se subdivide em módulos que serão apresentados abaixo:

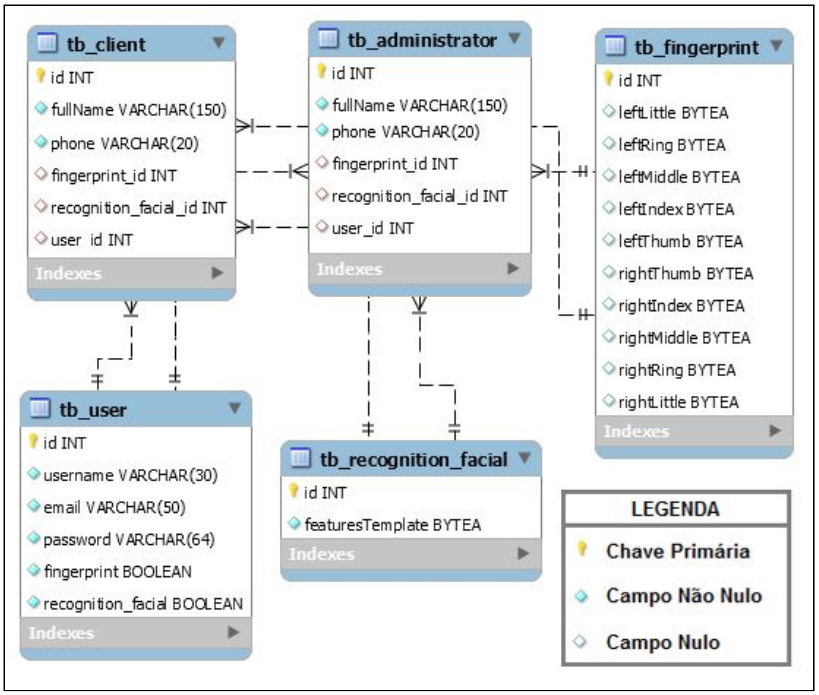
- *Persistence*: é responsável pelo armazenamento e recuperação de informações na base de dados, além de definir como esses dados serão armazenados. Ele abstrai a forma como são realizadas essas operações, fornecendo consultas personalizadas tanto para armazenamento, como também para a recuperação de informações.
- *Authentication*: compreende a camada responsável pela verificação das informações fornecidas pelos indivíduos com as armazenadas na base de dados, para comparar e verificar se essas informações são capazes de autenticar o indivíduo. Contém os algoritmos responsáveis por realizarem essas operações, bem como, permite a inclusão de autenticação através de novas categorias de reconhecimento biométrico. Este módulo é muito importante, pois é onde se encontram os algoritmos biométricos, que são fundamentais para a comparação dos dados e autenticação dos indivíduos.

Por questões de organização, as interfaces referentes aos módulos *Persistence* e *Authentication* são detalhadas no APÊNDICE A – INTERFACES DA API, fornecendo uma melhor visão de utilização da API.

3.2 DIAGRAMAS

Durante a construção do trabalho, fez-se necessário a construção de diagramas para facilitar a implementação da API, além de definir como os dados seriam armazenados.

Figura 11 – Diagrama Entidade-Relacionamento



Fonte: Elaborada pelo autor (2018).

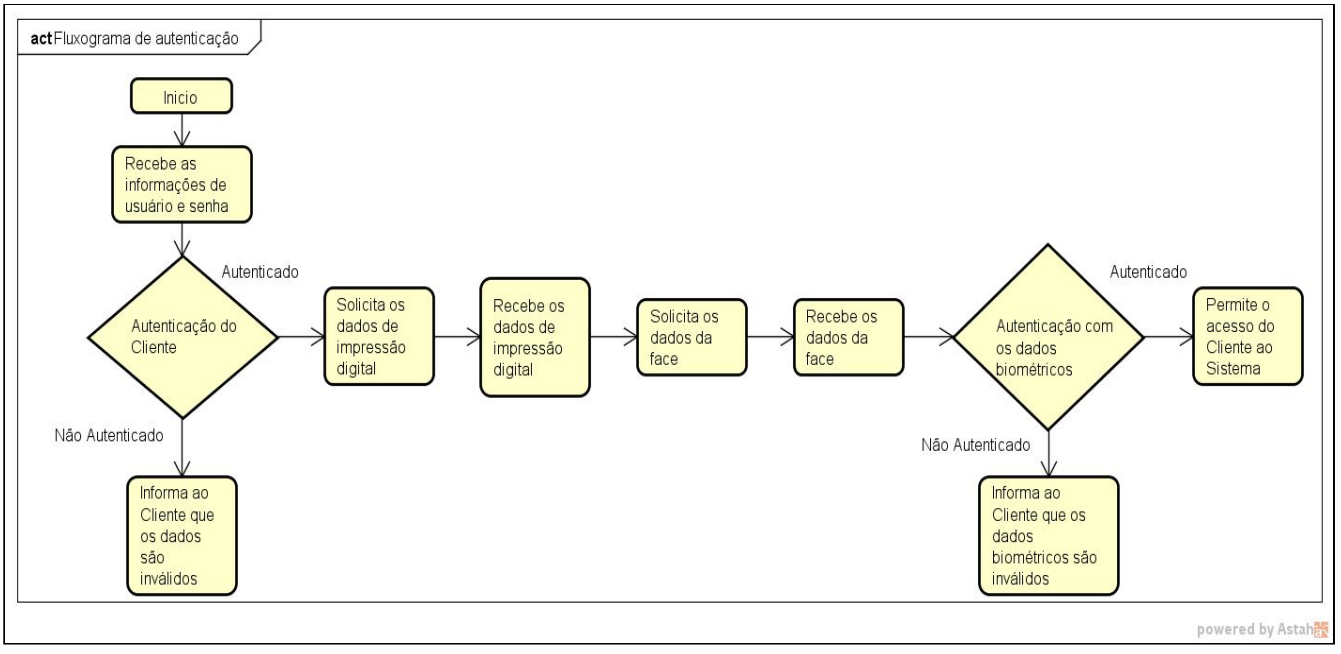
Na Figura 11, podemos observar o DER da base de dados da API, contendo 5 tabelas dentre elas: a tabela *tb_user* com os dados do usuário necessários para a autenticação por conhecimento, a *tb_fingerprint* que armazena os dados referentes as impressões digitais do usuário, a *tb_recognition_facial* que contém os dados referentes as características da face e as tabelas *tb_client* e *tb_administrator* que reúne todos os dados do usuário cadastrado, permitindo identificar quem tem permissão de administrador na aplicação, além de conter os dados como nome completo, data de nascimento e celular, os dados referentes ao usuário que estão presentes nas tabelas *tb_user*, *tb_fingerprint* e *tb_recognition_facial*.

3.3 DESCRIÇÃO DA APLICAÇÃO PROTÓTIPO

A aplicação protótipo integrará as autenticações baseadas em conhecimento e em características, utilizando login e senha juntamente com as categorias de reconhecimento biométrico de impressão digital e facial do indivíduo. A aplicação será desenvolvida para a plataforma *web* e utilizará a API de autenticação multibiométrica, se comunicando com os plug-ins para capturar as características biométricas no lado do cliente, para que esses dados sejam enviados para a aplicação no servidor processar e validar a autenticação do indivíduo.

Primeiramente, a aplicação solicitará dados como nome de usuário e senha, para iniciar o processo de autenticação do indivíduo. Caso esses dados sejam autenticados, será exibida uma página com informações referentes a captura de impressão digital, após a coleta desse dado será solicitado a captura da face do indivíduo. Por fim, se os dados biométricos coletados forem autenticados, o indivíduo poderá acessar o sistema, caso contrário será exibida uma mensagem de erro informando que os dados biométricos não são válidos para a autenticação do respectivo indivíduo.

Figura 12 – Fluxograma de Autenticação do Usuário



Fonte: Elaborada pelo autor (2018).

Como podemos observar no fluxograma de autenticação na Figura 12, o usuário precisa realizar todos os passos e caso o usuário seja autenticado, ele conseguirá acessar o sistema, onde conterá informações pessoas que foram utilizadas no seu cadastro.

3.4 MOCKUPS DAS TELAS

A seguir serão apresentados alguns protótipos de telas referentes a aplicação protótipo. Esses protótipos foram criados com base no uso da aplicação *web* pelo navegador, utilizando a ferramenta *Balsamiq Mockups*[19] que permite a criação de protótipos de interface gráfica de projetos de *software* oferecendo diversos recursos.

Na Figura 13 é apresentada a página inicial da aplicação, em que o usuário deverá informar o nome de usuário e a senha, nos respectivos campos, para iniciar o processo de autenticação baseado em conhecimento.

Figura 13 – Página Inicial do Protótipo

Fonte: Elaborada pelo autor (2017).

Após a autenticação com os dados informados inicialmente, será solicitado que o usuário coloque o dedo no sensor de leitura de impressão digital, configurado para se comunicar com a aplicação, para prosseguir com a autenticação baseado em características. Existe também a possibilidade de sair durante o processo de autenticação, voltando para a página inicial. A Figura 14 ilustra a página que solicita ao usuário que informe a impressão

[19] Disponível em: <https://docs.balsamiq.com/desktop/overview/>. Acesso em: 01/06/2017.

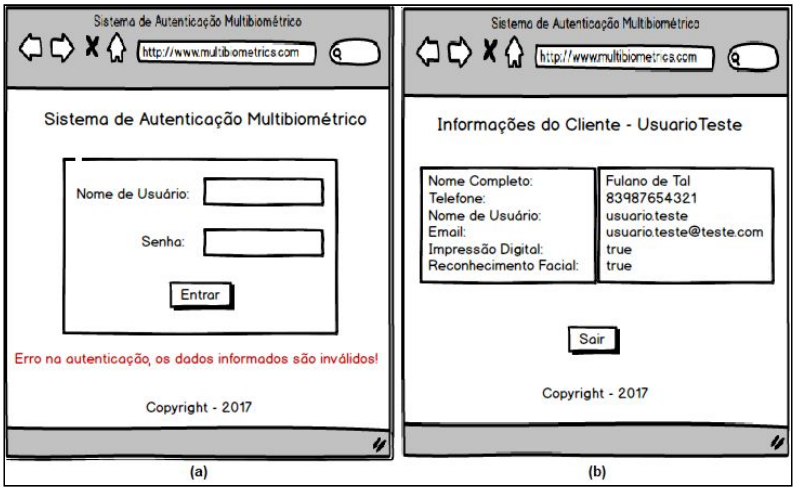
digital para prosseguir com o processo de autenticação, após informar a impressão digital, o último passo da autenticação é o reconhecimento facial. Na Figura 14 é ilustrada a página que solicita ao usuário que posicione a sua face na frente da câmera, de modo que seja possível reconhecer a sua face. É importante ressaltar que apenas o rosto do usuário esteja aparecendo na câmera, para que não ocorra erro no momento da autenticação.

Figura 14 – Autenticação por Impressão Digital e Facial

Fonte: Elaborada pelo autor (2017).

Após a captura dos dados biométricos, as informações serão verificadas realizando o processo de comparação e autenticação com os dados que estão armazenados na base. Depois dessas operações, haverá confirmação se o usuário foi autenticado, em caso negativo será informado que o usuário não pôde ser autenticado com base nos dados biométricos informados.

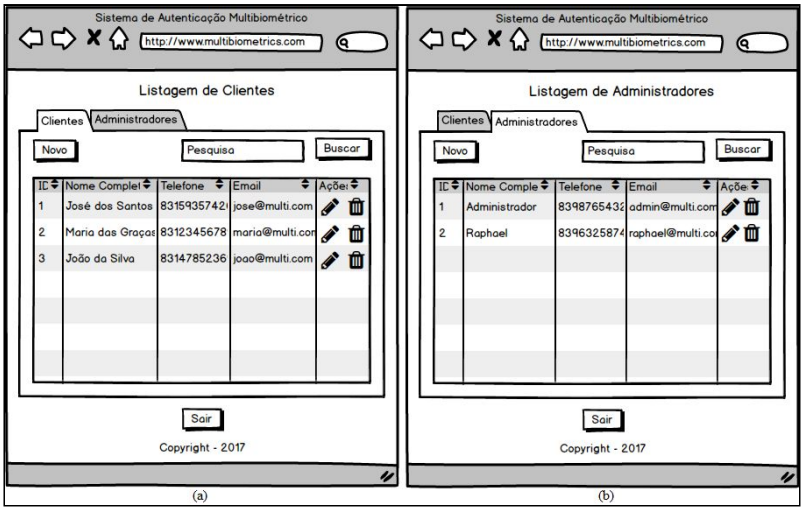
Figura 15 – Falha na Autenticação e Autenticação do Usuário



Fonte: Elaborada pelo autor (2017).

A Figura 15 ilustra a página de falha na autenticação devido aos dados biométricos serem inválidos, neste caso, se o usuário desejar acessar o sistema, ele deverá iniciar o processo de autenticação novamente. Já no caso em que o usuário foi autenticado através das biometrias fornecidas e se ele não tiver atributos de administrador, ele poderá visualizar as suas informações que estão na base de dados, como mostra a Figura 15. Após visualizar as informações, o usuário pode sair do sistema apertando o botão "Sair".

Figura 16 – Listagem de Clientes e Administradores

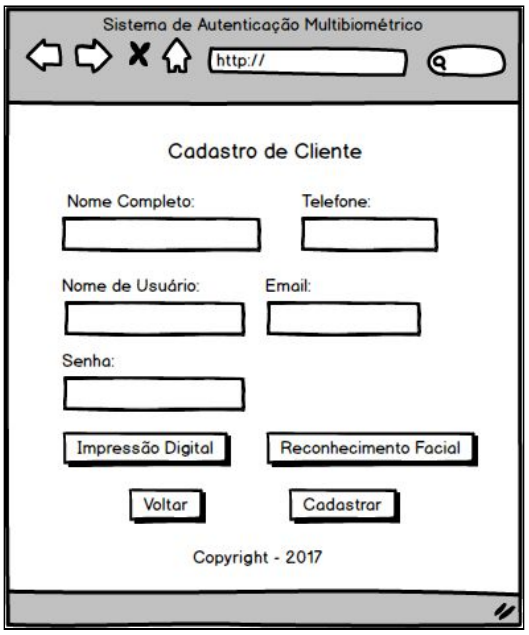


Fonte: Elaborada pelo autor (2017).

Caso o usuário que tenha sido autenticado possua atributos de administrador, ele será redirecionado para a página inicial do administrador. A Figura 16 mostra a página de listagem de clientes e administradores, nessas páginas o administrador poderá realizar operações de

cadastro de novos clientes ou administradores, além de permitir a busca, atualização e exclusão dos que já estão cadastrados na base. Na Figura 17 é exibida a página de cadastro de clientes, nela o administrador pode cadastrar um novo cliente, preenchendo os campos necessários e capturando as informações biométricas do indivíduo.

Figura 17 – Cadastro de Clientes



Fonte: Elaborada pelo autor (2017).

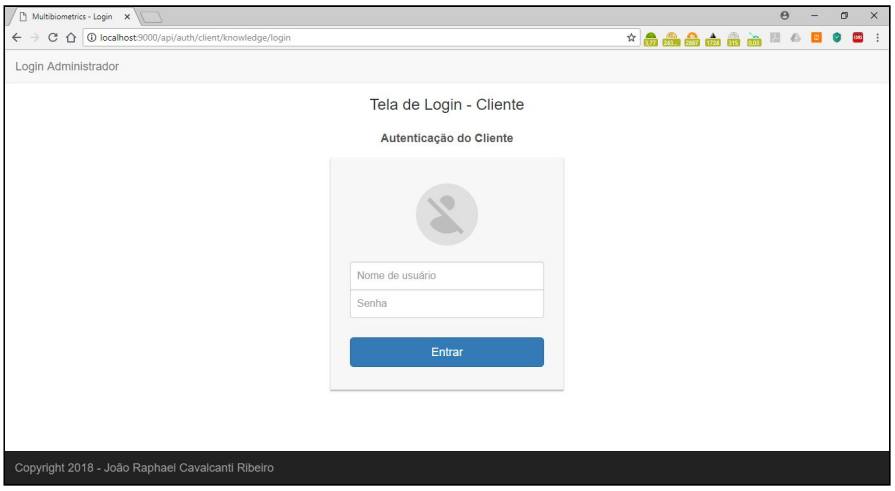
Esses *mockups* foram criados para facilitar o desenvolvimento das telas na aplicação protótipo, evitando que as telas não ficassem padronizadas e também para evitar muitas modificações após a criação delas.

3.5 TELAS DA APLICAÇÃO

A seguir serão apresentadas e descritas as principais telas da aplicação protótipo desenvolvida utilizando o *framework Bootstrap*[20] para a componentização da interface e *front-end*, que usa HTML, CSS e JavaScript.

[20] Disponível em: <https://getbootstrap.com/>. Acesso em: 25/06/2018.

Figura 18 – Tela de Login



Fonte: Elaborada pelo autor (2018).

Na Figura 18 – Tela de Login podemos observar a tela de login da aplicação onde o cliente deverá informar os dados de nome de usuário e senha para iniciar o processo de autenticação baseado em conhecimento.

Figura 19 – Tela de Captura da Impressão Digital

Fonte: Elaborada pelo autor (2018).

Após o cliente informar os dados necessário na tela de login, os dados são verificados e caso seja autenticado, seguirá para a captura da impressão digital, caso contrário retornará para a tela de login e será exibida uma mensagem de erro. Na Figura 19, podemos observar a tela de captura da impressão digital, nela é solicitado que o cliente insira o dedo no leitor de impressão digital para que as informações sejam capturadas e enviadas para a aplicação. Após

a captura, o botão “Próximo” será habilitado e o cliente poderá seguir com o processo de autenticação.

Figura 20 – Tela de Captura Facial

Fonte: Elaborada pelo autor (2018).

Na Figura 20, podemos observar a tela de captura facial, a imagem do lado esquerdo representa a captura em tempo real da câmera de vídeo, é necessário que o cliente pressione o botão “Capturar” para que a imagem do lado direito seja gerada. Após a captura da imagem, é aplicado o algoritmo para detecção facial, caso não seja detectado nenhuma face, é exibida a mensagem informando ao cliente que não foi detectada nenhuma face e que ele deve efetuar uma nova captura facial. Quando uma face for detectada, o botão “Próximo” será habilitado e o cliente poderá prosseguir com a autenticação.

Após o processo de captura facial, as informações biométricas serão verificadas e caso sejam autenticadas o cliente poderá visualizar as suas informações cadastradas na base de dados da aplicação. Caso as informações não sejam autenticadas, será exibida a tela de login informando que os dados biométricos são inválidos para autenticar o cliente.

Quando o cliente é autenticado e visualiza as suas informações cadastradas na aplicação, é permitido que ele altere as informações, além da possibilidade de habilitar e/ou desabilitar a autenticação por impressão digital e reconhecimento facial, desde que elas estejam cadastradas. Dessa forma, o cliente pode decidir quais as características biométricas serão utilizadas no processo de autenticação ao acessar a aplicação.

3.6 RESULTADOS OBTIDOS

O protótipo da aplicação pôde ser implementado utilizando a API de autenticação multibiométrica que foi proposta para esse trabalho, apenas utilizando as interfaces dos serviços fornecidos pela API e definindo o banco de dados que seria utilizado, de forma que a API não dependa unicamente de um banco de dados. A coleta das informações biométricas é através de um serviço *REST* que roda na máquina do cliente e que se comunica com os leitores, capturando essas informações e repassando para o protótipo, quando solicitadas.

Com relação aos testes de autenticação, foram capturadas impressões digitais e a face de 50 pessoas que forneceram as informações voluntariamente, foi possível cadastrar essas informações na aplicação protótipo e utilizar esses dados para verificar se a API funciona corretamente, impedindo que um indivíduo não autorizado acesse o sistema.

As autenticações através da impressão digital não obtiveram falhas, pois para que seja obtida é necessário que o dedo esteja em contato direto com o sensor, permitindo uma melhor confiabilidade na captura dessa informação e consequentemente na verificação com as informações cadastradas na base.

Já com relação as autenticações através do reconhecimento facial, apresentaram fatores que dificultaram a captura e/ou o reconhecimento facial, como a quantidade de luminosidade no ambiente de captura, a distância entre a câmera e o indivíduo e utensílios que o indivíduo estivesse usando como chapéu e óculos, além de evidenciar pontos negativos da captura facial, como a utilização de imagem da face de outra pessoa que foi posicionada em frente a câmera, seja através da imagem impressa em papel ou exibida no celular.

Com isso, a autenticação utilizando a impressão digital traz maior confiabilidade e autenticidade na sua utilização, enquanto a autenticação utilizando o reconhecimento facial vem como um segundo fator para que um indivíduo seja autenticado no sistema.

4 CONSIDERAÇÕES FINAIS

Este trabalho, até o momento, teve o intuito de desenvolver uma API capaz de fornecer algoritmos capazes de autenticar um indivíduo utilizando autenticação multibiométrica através de impressão digital e reconhecimento facial. Para utilização do protótipo da aplicação, faz-se necessário a utilização de sensores (leitor de impressão digital e câmera digital ou *webcam*), que auxiliam na captura dos dados biométricos do indivíduo, para que seja possível autenticá-lo.

Com relação aos objetivos propostos, foi possível identificar algumas das principais categorias de reconhecimento biométrico como: Impressão Digital, Face, Íris, Retina, Geometria da Mão, Geometria da Orelha, Voz e Assinatura (JAIN; ROSS; NANDAKUMAR, 2011; ZHANG; GUO; GONG, 2015). A partir da identificação, foram definidas a utilização das categorias de impressão digital e reconhecimento facial, devido ao custo/benefício com relação aos sensores e softwares utilizados na captura das informações biométricas. Após isso, foi desenvolvido a API de Autenticação Multibiométrica e implementado um protótipo de aplicação *web* utilizando a API.

Até o presente momento, foram realizadas pesquisas que permitiram compreender o processo de identificação de um indivíduo através das suas características biométricas, em especiais na impressão digital, reconhecimento facial e de íris, além do desenvolvimento de uma API de Autenticação Multibiométrica que utiliza reconhecimento facial e impressão digital, permitindo futuramente, a integração de novas categorias de reconhecimento. Durante o desenvolvimento do trabalho, foram criados diagramas e *mockups* de telas do protótipo da aplicação *web*, possibilitando uma visão evolutiva do desenvolvimento e facilitando o entendimento do fluxo de autenticação. Por fim, foi desenvolvida a aplicação protótipo que utiliza esta API para realizar o processo de autenticação utilizando as biometrias de impressão digital e facial, permitindo que os clientes visualizem os seus dados na aplicação.

As dificuldades observadas durante a elaboração do trabalho foi diante a definição das técnicas biométricas que seriam utilizadas no trabalho e além de dificuldades que surgiram durante o desenvolvimento da solução, como modelar a arquitetura da API para que permita a integração de novas categorias biométricas, definir a forma de comunicação entre os sensores

e a aplicação protótipo, além de compreender e implementar o processamento das informações biométricas. Apesar disso, as dificuldades foram superadas, através da utilização, testes e melhorias no desenvolvimento da API, implementação de um *plugin* na máquina cliente para comunicação com os sensores, além de prover um serviço que permita a coleta das informações biométricas e entender o funcionamento do processo de reconhecimento através de impressão digital e facial, para isso foram utilizadas API's de terceiros para processar as informações biométricas e permitir a autenticação dos indivíduos, através disso os objetivos foram alcançados.

Como proposta para trabalhos futuros, sugere-se a integração de novas técnicas de reconhecimento biométrico, bem como, a integração de autenticação baseada em propriedade, permitindo que a API de autenticação se torne mais completa e forneça vários modos de autenticação. Com relação a segurança dos dados armazenados, sugere-se a pesquisa sobre técnicas de armazenamento seguro dos dados biométricos, visto que por se tratar de uma característica intrínseca de uma pessoa, essa informação tem que ser tratada com um cuidado especial para que não seja acessada por pessoa não autorizadas. Também é possível pesquisar sobre algoritmos que detectem a vivacidade das características biométricas, permitindo identificar se a característica é de um ser vivo ou uma reprodução. Com relação a performance, é possível realizar testes para verificar o desempenho do uso da API em larga escala, considerando uma base de dados com um número significativo de usuários cadastrados.

REFERÊNCIAS

American National Standards Institute (ANSI). **Information Technology – Finger Image Based Data Interchange Format**. Disponível em: <http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+381-2009%5bR2014%5d>. Acesso em: 01/06/2017.

BEAL, A. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BRAGA, L. F. Z. **Sistemas de Reconhecimento Facial.** São Carlos: O Autor, 2013.

DEITEL, H. M.; DEITEL, P. J. **Java:** como programar. 6.ed. São Paulo: Pearson Prentice Hall, 2005.

Dlib C++ Library (DLIB). **High Quality Face Recognition with Deep Metric Learning.** Disponível em: <http://blog.dlib.net/2017/02/high-quality-face-recognition-with-deep.html>. Acesso em: 23/06/2018.

FONTES, E. L. G. **Segurança da Informação – O Usuário Faz a Diferença**. São Paulo: Saraiva, 2006.

GALTON, F. **Finger Prints**. London: MacMillan, 1892.

GALVÃO, M. C. **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education do Brasil, 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4.ed. São Paulo: Atlas, 2002.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à Segurança de Computadores.** Porto Alegre: Bookman, 2013.

HONG, L.; JAIN, A. K.; PANKANTI, S. **Can multibiometrics improve performance?** In: IEEE WORKSHOP ON AUTOMATIC IDENTIFICATION ADVANCED TECHNOLOGIES, 1999, New Jersey. p. 59-64.

HOUAISS, A.; VILLAR, M. S. **Dicionário Houaiss da língua portuguesa**, elaborado pelo Instituto Antônio Houaiss de Lexicografia e Banco de Dados da Língua Portuguesa S/C Ltda. 1.ed. Rio de Janeiro: Objetiva, 2009.

JAIN, A. K.; LI, S. Z. **Handbook of Face Recognition.** 2.ed. Editora Springer, 2011.

JAIN, A. K.; ROSS, A. A.; NANDAKUMAR, K. **Introduction to Biometrics.** Editora Springer, 2011.

MASCARENHAS, S. A. **Metodologia Científica.** São Paulo: Pearson Education do Brasil, 2012.

MORAES, A. F. **Segurança em Redes:** fundamentos. 1.ed. São Paulo: Érica, 2010.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Coorporativos.** São Paulo: Novatec Editora, 2007, p. 363-374.

NEHEMY, M. **Oftalmologia na prática clínica.** Belo Horizonte: Folium, 2015.

PEREIRA, L. F. A. **Detecção de impressões digitais falsas usando informações extraídas da rugosidade da pele.** 2013. 77 f. Dissertação (Mestrado em Ciência da Computação) – Centro de Informática, Universidade Federal de Pernambuco, Recife. 2013.

POSTGRESQL. **PostgreSQL 9.5.13 Documentation.** Disponível em: <https://www.postgresql.org/docs/9.5/static/index.html>. Acesso em: 01/06/2017.

RAKESH, T.; KHOGARE, M. G. **Survey of Biometric Recognition System for Iris**. In: International Journal of Emerging Technology and Advanced Engineering, 2., 2012, Ambajogai, India. p. 272-276.

RATHA, N. K.; SENIOR, A. W.; BOLLE, R. M. **Automated biometrics**. In: INT. CONF. ADVANCES PATTERN RECOGNITION, 2001, Rio de Janeiro, Brazil. p. 445-454.

ROSS, A. A.; NANDAKUMAR, K.; JAIN, A. K. **Handbook of Multibiometrics.** New York: Springer, 2006. 198 p. (International Series on Biometrics).

SILVA, A. A.; GOMIDE, C. F.; PETRILLO, F. **Metodologia e projeto de software orientados a objetos:** modelando, projetando e desenvolvendo sistemas com UML e componentes distribuídos. São Paulo: Érica, 2003.

YOUNG, H. D.; FREEDMAN, R. A. **Física IV:** ótica e física moderna. São Paulo: Addison Wesley, 2009.

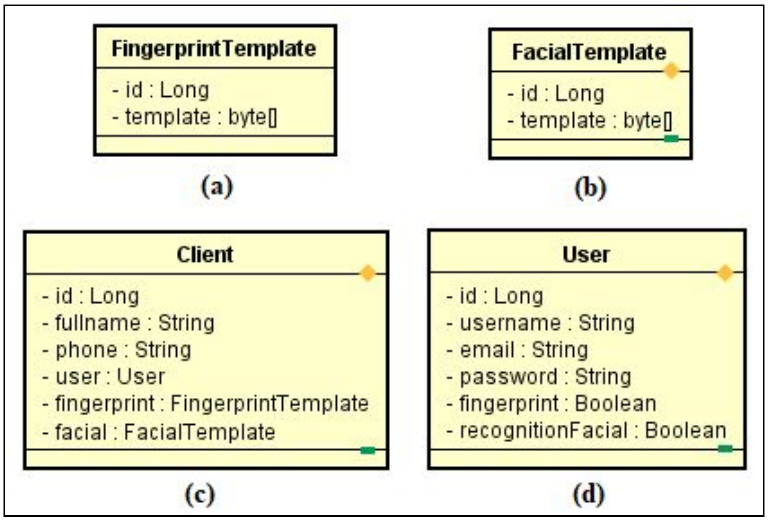
ZHANG, D.; GUO, Z.; GONG, Y. **Multispectral Biometrics:** Systems and Applications. Editora Springer, 2015.

APÊNDICE A – INTERFACES DA API

A.1. TIPOS DE DADOS

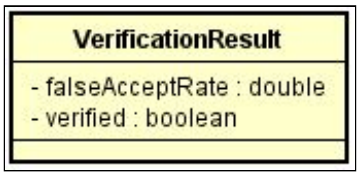
Os tipos de dados que fazem parte dos módulos *Persistence* e *Authentication*, que constituem a API do componente *Multibiometrics*, são apresentadas a seguir:

Figura 21 – Tipos de Dados



A Figura 21 representa quatro tipos de dados utilizados pela API, o *FingerprintTemplate* que armazena as informações referentes ao *template* de impressão digital e o *FacialTemplate* que armazena as informações do *template* da face, ambos contêm os atributos *ID* que é do tipo *Long* como identificador único do registro no banco de dados e o atributo *template* que é um *array* de *bytes* que armazena as informações das características biométricas capturadas. Já o *Client* armazena as informações referentes ao cliente, contendo informações pessoais, biométricas e de autenticação, e o *User* que contém as informações utilizadas para autenticação do cliente, como nome de usuário (*username*), e-mail, senha (*password*) e quais as categorias biométricas serão utilizadas para autenticação do cliente na aplicação.

Figura 22 – Tipo de Dado Verification Result



Na Figura 22, consta o objeto *VerificationResult* que armazena o resultado de uma verificação com informações biométricas. Contém os campos *falseAcceptRate* do tipo *double* que indica a taxa de falsa aceitação que é a diferença entre um *template* armazenado na base com um utilizado para verificação e o campo *verified* que é um booleano que informa se os dados utilizados na verificação são compatíveis e pertencentes à mesma pessoa.

A.2. INTERFACE PERSISTENCE

As operações que fazem parte do módulo *Persistence* são apresentadas a seguir.

Tabela 1 – Especificação da operação insertClient (client)

Client	insertClient (client)
Esta operação inclui, no banco de dados, um novo cliente que receberá um ID único.	
Parâmetros:	**cliente:** objeto com as informações de um cliente.
Retorno:	Esta operação retorna um objeto Client com as informações armazenadas na base de dados.
Exceções:	

Tabela 2 – Especificação da operação updateClient (client)

Client	updateClient (client)
Esta operação atualiza, no banco de dados, as informações de um cliente já cadastrado.	
Parâmetros:	**cliente:** objeto com as informações de um cliente que serão atualizadas.
Retorno:	Esta operação retorna um objeto Client com as informações armazenadas na base de dados.
Exceções:	

Tabela 3 – Especificação da operação findClientById (id)

Client	findClientById (id)

Esta operação realiza a consulta, no banco de dados, de um cliente através do seu valor correspondente ao identificador.	
Parâmetros:	**id:** valor inteiro correspondente ao identificador do cliente no banco de dados da aplicação.
Retorno:	Esta operação retorna um objeto Client com as informações armazenadas na base de dados.
Exceções:	**InvalidClientIdException:** o identificador do cliente é inválido.

Tabela 4 – Especificação da operação removeClientById (id)

Void	removeClientById (id)
Esta operação exclui, do banco de dados, um cliente cadastrado através do seu número correspondente ao identificador.	
Parâmetros:	**id:** valor inteiro correspondente ao identificador do cliente no banco de dados da aplicação.
Retorno:	Esta operação não retorna nenhum valor (*void*).
Exceções:	**InvalidClientIdException:** o identificador do cliente é inválido.

A.3. INTERFACE AUTHENTICATION

As operações que fazem parte do módulo *Authentication* são apresentadas a seguir.

Tabela 5 – Especificação da operação authenticate (username, password)

boolean	authenticate (username, password)
Esta operação realiza a comparação entre as informações passadas por parâmetro e as que estão no banco de dados, verificando se é possível autenticar o cliente.	
Parâmetros:	**username:** *String* referente ao nome de usuário do cliente na aplicação. **password:** *String* referente a senha do cliente na aplicação.
Retorno:	Esta operação retorna o valor *true* se as informações são válidas ou *false* caso não sejam válidas.
Exceções:	

Tabela 6 – Especificação da operação matchFingerprint (client, fingerprint)

VerificationResult	matchFingerprint (client, fingerprint)
Esta operação realiza a comparação entre as informações passadas por parâmetro e as que estão no banco de dados, verificando se é possível autenticar o cliente através da impressão digital.	
Parâmetros:	**client:** *Client* referente as informações do cliente que realizará o processo de autenticação por impressão digital. **fingerprint:** *FingerprintTemplate* com as informações de impressão digital capturada para autenticação.

Retorno:	Esta operação retorna um *VerificationResult* referente ao resultado do processo de autenticação por impressão digital.
Exceções:	

Tabela 7 – Especificação da operação matchRecognitionFacial (client, facial)

VerificationResult	matchRecognitionFacial (client, facial)
Esta operação realiza a comparação entre as informações passadas por parâmetro e as que estão no banco de dados, verificando se é possível autenticar o cliente.	
Parâmetros:	**client:** *Client* referente as informações do cliente que realizará o processo de autenticação por reconhecimento facial. **facial:** *FacialTemplate* com as informações da face capturada para autenticação.
Retorno:	Esta operação retorna um *VerificationResult* referente ao resultado do processo de autenticação por reconhecimento facial.
Exceções:	