

FGP – FACULDADE G&P

Sistemas de Informação

**RECONHECIMENTO FACIAL VOLTADO A SEGURANÇA
DE CAIXAS ELETRÔNICOS**

Heder L. Silva

Richard J. Algarve

Pederneiras - SP

2014

FGP – FACULDADE G&P

Sistemas de Informação

**RECONHECIMENTO FACIAL VOLTADO A SEGURANÇA
DE CAIXAS ELETRÔNICOS**

Heder L. Silva

Richard J. Algarve

**Trabalho apresentado como requisito obrigatório
à conclusão do Curso de Bacharelado de Sistemas
de Informação da Faculdade G&P.**

Orientador: Prof. Ms. Anderson Francisco Talon

Pederneiras – SP

2014

Folha de Aprovação

Pederneiras, 01 de Dezembro de 2014.

Orientador: Prof. MS. Anderson Francisco Talon _____

Examinador 1: Prof. MS. André Marcelo Farina _____

Examinador 2: Prof. Fernando de Sousa Faria_____

Dedico esta pesquisa a ilustres pessoas que contribuíram direta ou indiretamente para a conclusão da mesma, em especial: A minha esposa Lucinéia a qual contribuiu com paciência e compreensão em momentos nos quais estive ocupado em pesquisas. A minha filha Heloísa pelos momentos que estive ausente das brincadeiras e afetos sendo estes de grande importância para a evolução intelectual de uma criança. Aos meus pais que nas terças-feiras vinham me visitar sempre trazendo conselhos de mestre para que eu pudesse viver e compreender que as dificuldades da vida são fonte de aprendizagem para a evolução do espírito. Aos meus amigos e familiares que acreditaram no potencial significativo desta pesquisa. A Deus que me deu força para prosseguir mesmo com críticas não construtivas as quais eram voltadas a este estudo científico. E em último lugar, mas não o menos significativo, o meu amigo Heder Lopes que aceitou meu convite para enfrentar este estudo com responsabilidade e dedicação sempre se mostrando empenhado na busca de novas informações.

RICHARD J. ALGARVE

Dedico este trabalho em primeiro lugar a Deus que iluminou o meu caminho durante esta caminhada. Aos meus pais, Hercules Lopes e Ana Cintra, minhas irmãs, Débora Lopes e Lívia Cintra, e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida. Ao meu amigo Richard J. Algarve por não ter medido esforços para que juntos concluíssemos este trabalho. Dedico também a todos os professores que me acompanharam durante a graduação contribuindo com minha formação profissional e pessoal, tornando possível a realização deste trabalho. Por fim aos amigos e colegas, pelo incentivo e pelo apoio constante.

HEDER L. SILVA

AGRADECIMENTOS

Agradecemos a todos que direta ou indiretamente contribuíram para a conclusão desta pesquisa: Primeiramente agradecemos a equipe de docentes que nos acompanharam e com agradecimentos especiais para nosso professor e orientador professor Ms. Anderson Francisco Talon, o qual, por questões de experiência, compreendeu nossos problemas, limitações e angustias e a nossa coordenadora do curso de sistemas de informação, professora Ms. Vânia Somaio Teixeira, a qual forneceu, através de preciosas palavras, incentivo para aceitarmos que todo resultado tem extrema importância para a evolução de um projeto. Agradecemos a empresa G&P na qual trabalhamos como desenvolvedor de software, pois a mesma nos apoiou com compreensão nos momentos que precisávamos de maior foco nesta pesquisa. E por fim agradecemos a nossas famílias e amigos pelo incentivo e amparo nos momentos de ansiedade com o cumprimento deste precioso estudo.

“A curiosidade é mais importante do que o conhecimento.”

ALBERT EINSTEIN

RESUMO

Atualmente as instituições bancárias vêm sendo alvo de constantes fraudes envolvendo cartões de crédito e débito, quando utilizados em caixas eletrônicos. Desta forma as instituições necessitam investir bilhões de reais para garantir a segurança dos usuários que acessam caixas eletrônicos. Características biológicas são utilizadas para promover mecanismos de identificação e controles de acessos a locais e sistemas que requerem tais controles. O objetivo deste trabalho busca adquirir conhecimento sobre técnica de reconhecimento facial, que é o uso das características da face de um indivíduo, verificando a viabilidade de utilizá-la como complemento do uso do cartão e da senha. Para complementar os dados obtidos através do referencial teórico foi desenvolvido um protótipo com intuito de demonstrar a técnica de reconhecimento facial. Por fim, alguns testes foram realizados com o protótipo para análise da viabilidade de implantação da técnica em caixas eletrônicos.

Palavras-chaves: Reconhecimento Facial; Biometria; Caixas eletrônicos; Fraudes em cartões.

ABSTRACT

Currently banking institutions have been subject to constant fraud involving in credit and debit cards, when used at ATMs. Then these institutions need to invest billions of reais to ensure the safety of users accessing the ATMs. Biological characteristics are used to promote mechanisms to identify and access the systems that require this type of control. This study try to get technical knowledge about facial recognition, checking the viability of using it as a complement to card and PIN. To complement the data obtained through the theoretical referential was developed a prototype to demonstrate the technique of facial recognition. Finally, some tests were performed with the prototype to analyze the viability of the technique in ATMs.

Keywords: Facial Recognition; biometrics; ATMs; Fraud on cards.

LISTA DE ILUSTRAÇÕES

Figura 1 - Transação em caixa eletrônico.....	21
Figura 2 - Cartão Magnético.....	21
Figura 3 - Dispositivos utilizados em clonagem de cartões.	23
Figura 4 - “chupa-cabra”	25
Figura 5 - Exemplo do uso de um sistema biométrico.	28
Figura 6 - Pontos indentificadores das digitais.....	32
Figura 7 - Íris	34
Figura 8 - Exemplo Retina.....	34
Figura 9 - Principais operações biométricas: autenticação (verificação) e identificação (reconhecimento).	37
Figura 10 - Distribuição fictícia de falsos positivos e falsos negativos estabelecidos através de um limiar.	39
Figura 11 - Exemplo de dimensões de uma imagem.....	41
Figura 12 - Área da imagem com uma região de interesse ampliada.....	41
Figura 13 - Valor de Corte = 127 Fonte - Mello (2014).....	43
Figura 14 - Exemplo da arquitetura de um sistema de reconhecimento facial.....	47
Figura 15 - Características de <i>Haar</i> utilizadas na detecção facial.....	49
Figura 16 - Padrões faciais encontrados com base em contrastes.	49
Figura 17 - Geração da imagem integral.	50
Figura 18 - Detecção facial em vídeo.....	51
Figura 19 - Semelhança entre imagens originais e imagens processadas após aplicação de PCA.	53
Figura 20 - Representação do processo de cadastrar senha e treinamento de faces.	58
Figura 22 - Representação da tentativa de acesso por um impostor.....	60
Figura 24 - Diagrama do banco de dados utilizado no protótipo.	67
Figura 25 - Tela de cadastro do módulo administrativo.....	68
Figura 26 - Aguardando Captura.....	69
Figura 27 - Aguardando Face.	69
Figura 28 - Face sendo detectada.	69
Figura 29 - Duas faces Sendo detectadas.	70
Figura 30 - Aguardando Detecção da Face	70
Figura 31 - Área de região de interesse da face.....	71

Figura 32 - Tela de Consulta do Módulo Administrativo	72
Figura 33 - Resultado da consulta de clientes	72
Figura 34 - Tela Inicial do Modulo Operacional	73
Figura 35 - Tela para inserção da senha	73
Figura 36 - Imagem do protótipo aguardando face para o reconhecimento.....	74
Figura 37 - Momento em que a comparação é realizada	75
Figura 38 - Menu de operações disponibilizado após permissão de acesso.....	75
Figura 39 - Exemplo de comparação feita na tentativa de acesso	84
Figura 40 - Segundo exemplo de comparação.....	84
Figura 41 - Amostragem do tempo de detecção de uma face em uma imagem	86

LISTA DE TABELAS

Tabela 1 - Comparação de fraudes em cartões em relação a outras fraudes.	27
Tabela 2 - Comparação entre os tipos de biometria.	31
Tabela 3 - Parâmetros resultantes do teste de configuração do protótipo.	77
Tabela 4 - Teste com o voluntário Felipe Costa.	78
Tabela 5 - Teste com o voluntário Gustavo Pinheiro.	78
Tabela 6 - Teste com o voluntário Lucas Soto.	79
Tabela 7 - Teste com o voluntário Glauco.	79
Tabela 8 - Teste com o voluntário Heder Lopes.	80
Tabela 9 - Teste com o voluntário Richard Algarve.	80
Tabela 10 - Teste com o voluntário Douglas Ferreira.	81
Tabela 11 - Teste com o voluntário Daniel Simões.....	81
Tabela 12 - Teste com o voluntário Carlos Piva.	82
Tabela 13 - Teste com o voluntário Claudiney Pereira.	82
Tabela 14 - Testes com acessórios 1.	83
Tabela 15 - Teste com acessórios 2.....	84
Tabela 16 - Teste com gêmeas idênticas 1.	85
Tabela 17 - Testes com gêmeas idênticas 2.....	85
Tabela 18 - Tempo médio para reconhecimento.	86
Tabela 19 - Comparação dos pontos favoráveis e desfavoráveis.	87

LISTA DE ABREVIATURAS E SIGLAS

ABECS: Associação Brasileira das Empresas de Cartões de Crédito e Serviços.

ARISP: Associação dos Registradores Imobiliários de São Paulo.

CPP: Centro de Políticas Públicas.

FEBRABAN: Federação Brasileira de Bancos.

IBM: *International Business Machines*.

INSPER: Instituto de Ensino e Pesquisa.

PROCON: Programa de Orientação e Proteção ao Consumidor.

PCA: *Principal Component Analysis*.

ROI: *Region of interest*.

OPENCV: *Open Source Computer Library*.

LBP: *local Binary Pattern*.

IA: Inteligência artificial.

SUMÁRIO

1.	INTRODUÇÃO	15
1.1.	Problema	17
1.2.	Objetivos	17
1.2.1.	Objetivos Gerais	17
1.2.2.	Objetivos Específicos	17
1.3.	Justificativas.....	18
1.4.	Metodologia de pesquisa	18
1.5.	Organização do trabalho	18
2.	FRAUDES EM CAIXAS ELETRÔNICOS	20
2.1.	Caixa eletrônico	20
2.2.	Cartões Magnéticos.....	21
2.3.	<i>Smart Cards</i>	22
2.4.	Vulnerabilidade dos cartões e caixas eletrônicos.....	22
2.4.1.	Fraude “Troca de Cartões”	24
2.4.2.	Fraudes ocasionadas por descuidos do usuário	24
2.4.3.	Fraudes através dos <i>Credit Card Skimming</i> ou “chupa-cabras”.....	24
2.4.4.	Fraudes em <i>Smart Cards</i>	25
2.5.	Estatísticas sobre as fraudes.....	26
2.6.	Bancos e o investimento em segurança biométrica	28
3.	IDENTIFICAÇÃO BIOMÉTRICA	29
3.1.	Aplicação da Biometria.....	29
3.2.	Requisitos da Biometria.....	30
3.3.	Tipos de Biometria.....	31
3.3.1.	Biometria Fisiológica	31
3.3.2.	Biometria Comportamental	35
3.4.	Modos de operação para biometria.....	36
3.5.	Desempenho dos sistemas biométricos.....	37
4.	PROCESSAMENTO DE IMAGENS E VISÃO COMPUTACIONAL	40
4.1.	O que é uma imagem a nível computacional?	40
4.2.	Processamento de imagem.....	42
4.3.	Limiarização	43

4.4.	Histogramas	43
4.5.	Equalização de Histogramas	44
4.6.	Visão Computacional.....	45
5.	RECONHECIMENTO FACIAL	46
5.1.	Sistema de reconhecimento facial.....	46
5.2.	Detecção facial.....	48
5.3.	Extração de características.....	51
5.3.1.	PCA através da abordagem <i>Eigenfaces</i>	52
5.4.	<i>Frameworks</i> para reconhecimento facial	55
5.5.	OpenCV	55
5.6.	EmguCV	56
6.	PLANEJAMENTO DO PROTÓTIPO.....	57
6.1.	Módulo Administrativo.....	57
6.2.	Módulo Operacional	58
6.3.	Estudos de Caso	59
6.3.1.	Problema do roubo de identidade (clonagem do cartão)	59
6.3.2.	Esquecimento de senha.....	60
6.3.3.	Perda do cartão	61
6.3.4.	Falsos negativos decorrentes de alterações faciais	62
6.3.5.	Falsos positivos decorrentes de semelhanças faciais.....	62
6.3.6.	Auxílio de um terceiro para realizar transações no caixa-eletrônico.....	62
6.4.	Adequação da infraestrutura para o reconhecimento facial	63
6.5.	Delimitações da solução proposta.....	63
6.6.	Configuração do protótipo	63
6.7.	Coleta de dados	64
7.	DEMONSTRAÇÃO DAS FUNCIONALIDADES DO PROTÓTIPO	66
7.1.	Demonstração das funcionalidades Protótipo	66
7.1.1.	Funcionalidades do módulo administrativo	67
7.1.2.	Funcionalidades do módulo operacional	72
8.	RESULTADOS OBTIDOS COM A COLETA DE DADOS.....	76
8.1.	Configuração do Protótipo.....	76
8.2.	Resultados do Protótipo	77
8.3.	Testes Adicionais (Barba e Óculos).....	83

8.4.	Teste Adicional (Gêmeas).....	85
8.5.	Verificação do tempo de detecção de face e do reconhecimento facial.	86
9.	CONCLUSÃO	87
9.1.	Implementações Futuras	88
	REFERÊNCIAS	89
	APÊNDICES	96

1. INTRODUÇÃO

Um indivíduo pode ser identificado por diversas características físicas, contudo a mais marcante é a face, permitindo que uma pessoa seja distinguida em meio a outras. Tal habilidade é para o ser humano a clara presença de estímulos cognitivos provenientes de uma região do cérebro denominada área fusiforme da face, a qual segundo Juste (2006), está localizada na parte posterior inferior do cérebro, permitindo identificar faces através da atenção e memória. No intuito de atribuir características que simulem esta área do cérebro nos computadores, surgiram vários estudos voltados à inteligência artificial (IA).

Segundo Lopes (2014), a inteligência artificial está com um crescente sucesso na simulação da inteligência humana e ao contrário do que muitos pensam a mesma não se limita apenas a atividades intelectuais tais como raciocínio matemático e linguagem, podendo compreender atividades mais intuitivas tais como andar, comer e ver. Lopes (2014), também afirma que a visão computacional é uma subárea da IA cujo principal objetivo é a criação de um sistema de visão artificial que simule o sistema visual humano.

Para Lopes (2014), o desenvolvimento de equipamentos computacionais mais rápidos tem promovido notórios avanços na área de visão computacional e os sistemas de reconhecimento facial, através de vídeo ou imagens estáticas, estão se tornando realidade.

Medeiros (2012) afirma que cada vez mais as pessoas se interessam por sistemas de segurança cujas finalidades podem ser representadas pelo controle de acesso de indivíduos em áreas restritas, assim como é dissertado nesta pesquisa. Um dos usos do reconhecimento facial pode ser exemplificado pelo filme *Minority Report* (2002), onde o personagem John Anderton (Tom Cruise) é reconhecido por características faciais, ao passar por anúncios holográficos.

Diante o cenário pesquisado é explorado a segurança dos bancos e seus caixas eletrônicos os quais podem ser inseguros para os clientes. Tal insegurança é comprovada por notícia publicada pelo Jornal Nacional (2009), informando um aumento de 43% nos índices de clonagem de cartão. Nos dias atuais estes índices estão muito maiores; segundo Relatório da Pesquisa de Vitimização em São Paulo divulgado pela INSPER (2013), nos anos de 2003 até 2013 houve um aumento de 327,5% em fraudes com cartões de crédito.

Partindo-se do princípio de que, para obter um grau satisfatório de segurança, depende-se de um conjunto de medidas previamente adotadas, e não de uma ação isolada, conforme descrito no dicionário *online* de conceitos, QueConceito (2014, Conceito de segurança).

“A segurança é um conjunto de medidas assumidas para proteger-se de quaisquer atos de violência, como pode ser ataques, roubos, espionagens, sabotagens, etc. A segurança implica a qualidade ou o estado de estar seguro. Com a seguridade se tenta evitar as exposições a situações perigosas e a devida atuação para estar protegido diante de situações adversas.”

Com base nesse conceito, a segurança dos serviços bancários por intermédio dos caixas eletrônicos, depende de várias medidas assumidas por parte das instituições financeiras, como constantes investimentos em novas tecnologias ou desenvolvimento de novos procedimentos, além do cuidado dos usuários durante a utilização de algum serviço.

Apesar do Superior Tribunal de Justiça (2011) afirmar que os clientes devem ser resarcidos pelo banco, segundo Lordello (2014), especialista em segurança pública e privada, a pessoa que já foi vítima de uma fraude em um caixa eletrônico passa por grande infelicidade, pois além dos prejuízos financeiros momentâneos, são alvos da própria inexperiência, permitindo torná-las um alvo fácil, para o que Lordello (2014) denomina “arapuca” de criminosos, ou seja, as armadilhas utilizadas pelos criminosos para fraudar o sistema bancário.

Visando explorar o uso do reconhecimento facial voltado a segurança, foi pesquisado o notório auxílio desta tecnologia quando associada aos dispositivos de automação bancária (Caixas Eletrônicos), permitindo que os correntistas possam ter novas opções de segurança, assegurando também as instituições bancárias, pois estas sofrem prejuízos mesmo com altos investimentos.

Diante da necessidade de reduzir índices de clonagem de cartões, sendo que a tecnologia smart card (CHIP), como dito por Zmoginski (2007) do Portal Info, não é totalmente segura quanto à fraude, é proposto o uso do reconhecimento facial para evitar que indivíduos não autorizados façam uso de contas de reais correntistas, garantindo a autenticidade dos mesmos.

Para complementar a dissertação de conclusão de curso, comprovando a mesma, foi desenvolvido um protótipo, inicialmente denominado *KeyFace*, o qual engloba os processos de autenticação vigentes em um caixa eletrônico, em específico as senhas, juntamente com o reconhecimento facial. Tal protótipo está voltado à autenticação do correntista evitando que pessoas não autorizadas façam uso de uma conta a qual não são titulares e ao mesmo tempo armazenar um histórico de faces que estiveram envolvidas na transação, para que em caso de possível fraude o banco tenha informações para constatar a mesma.

O *KeyFace* foi desenvolvido em C# .NET, linguagem mantida pela Microsoft, fazendo uso da técnica PCA (*Principal Component Analysis*) contida no framework OpenCV. Outras técnicas serão utilizadas e descritas futuramente ao longo do desenvolvimento desta monografia.

1.1. Problema

Segundo orientação da Fundação PROCON de São Paulo aos usuários de Cartões de Crédito, por intermédio do Guia Cartão de Crédito (2014); os cartões de crédito e/ou débito e suas respectivas senhas são intransferíveis e de uso pessoal, desta forma, somente o titular pode realizar operações bancárias com o mesmo. Apesar de, as instituições financeiras investirem pesado em segurança eletrônica, que é de cerca de R\$ 9,4 bilhões, três vezes superiores ao valor do início da década, conforme anúncio no *Home Page* da FEBRABAN (2014), as formas de autenticação que existem, não impedem que outra pessoa de posse do cartão do titular da conta, efetue uma transação bancária não autorizada.

1.2. Objetivos

A seguir estão relacionados os objetivos gerais e específicos deste trabalho.

1.2.1. Objetivos Gerais

Os objetivos gerais são possibilitar um maior conhecimento e divulgação diante o uso de técnicas de visão computacional para aumentar a segurança dos caixas eletrônicos de forma complementar, ou seja, auxiliando as técnicas de segurança já existentes.

1.2.2. Objetivos Específicos

Os objetivos específicos são:

- Demonstrar através de um protótipo o ganho de segurança promovido pelo uso de técnicas de reconhecimento facial.
- Mensurar o tempo de execução do algoritmo de reconhecimento facial, que compreende entre a captação da imagem até o reconhecimento e verificação da face.

- Verificar se o tempo de execução do algoritmo irá tornar a técnica de reconhecimento facial viável para se implantar como forma de validação em um caixa eletrônico.
- Fazer um levantamento dos índices de falsos positivos e falsos negativos gerados pelo algoritmo, para análise de viabilidade de sua implantação.

1.3. Justificativas

Existe um aumento constante no percentual de fraudes em caixas eletrônicos, o que causa transtornos e sensação de insegurança nos usuários dos serviços bancários, oferecidos por intermédio dos caixas eletrônicos, causando prejuízos financeiros, pois é de responsabilidade dos bancos o resarcimento aos usuários, caso haja constatação da fraude. Cria então nos bancos, uma necessidade permanente de investimento em novas tecnologias ou desenvolvimento de novos procedimentos, com intuito de minimizar os prejuízos, trazer segurança a seus clientes e a manutenção de sua marca, pela qual o banco se estabelece no mercado.

1.4. Metodologia de pesquisa

Para o desenvolvimento deste trabalho foi realizada pesquisa bibliográfica baseada em livros, artigos científicos, documentários e publicações na internet. Como complemento, foi realizada uma pesquisa experimental através do desenvolvimento de um protótipo para o melhor entendimento da técnica de reconhecimento facial.

1.5. Organização do trabalho

Após a introdução do trabalho que foi feita no primeiro capítulo, no segundo capítulo foi feito levantamento das fraudes relacionadas aos caixas eletrônicos. Foi feito a constatação das fraudes e as formas que elas ocorrem.

No terceiro capítulo foram feitos estudos sobre os tipos de identificação biométrica, formas que se aplica a biometria, seus requisitos e os tipos de biometria existentes.

No quarto capítulo foi feito um estudo sobre processamento de imagens, tendo em vista que o reconhecimento facial que é o tipo de biometria utilizada neste trabalho, é uma vertente do processamento de imagens. Este capítulo foi necessário para compreender o que é uma imagem, conceitos de limiarização e equalização de histogramas.

No quinto capítulo foi tratado o reconhecimento facial. Foi feita uma descrição de como ocorre a detecção de uma face em uma imagem, a extração de características com PCA através da abordagem *Eigenfaces* e os tipos de frameworks para o reconhecimento facial.

No sexto capítulo é feita a descrição do planejamento do protótipo. Foram feitos estudos de caso de algumas situações pudessem ocorrer com o protótipo, a delimitação do tema proposto, a observação de alguns parâmetros que devem ser observados no momento da utilização do protótipo e a forma e ocorreu a coleta de dados.

No sétimo capítulo foram demonstradas as funcionalidades dos módulos dos protótipos, tanto administrativo como operacional.

No oitavo capítulo foram demonstrados os resultados obtidos com os testes realizados com o protótipo.

No último capítulo é feito o fechamento do trabalho. Neste capítulo é feita a conclusão do trabalho baseada nos testes realizados com o protótipo.

2. FRAUDES EM CAIXAS ELETRÔNICOS

Este capítulo tem como objetivo descrever a problemática de roubo de identidade, que é como se denomina as fraudes em cartões de débito e crédito envolvendo bancos e clientes. Serão descritas as formas que criminosos subtraem dados de cartões de correntistas, os objetivos dos criminosos com a subtração de dados e as consequências geradas por estas modalidades de fraudes.

Primeiramente será feita uma breve descrição de como funciona um caixa eletrônico, posteriormente uma síntese das características dos cartões de tarja magnética e também dos cartões de “chip”, denominados *smart cards*. Esta descrição não tem como objetivo aprofundar-se especificamente nos dispositivos citados, por não ser o foco central da pesquisa, mas por estarem relacionados às fraudes, irão fornecer subsídios para expô-las e desta forma relacioná-las as soluções que serão propostas nos capítulos posteriores.

2.1. Caixa eletrônico

Os primeiros caixas eletrônicos aceitavam apenas uma ficha, que era retida pelo caixa. Essa trabalhava com o princípio de magnetismo de baixa coercitividade (baixa densidade da camada magnética), o que a torna mais suscetível a rasuras, conforme informações da Cardcom (2014). O magnetismo presente na ficha era retirado pelo leitor de cartão para tornar fraudes mais difíceis.

Na atualidade as tecnologias bancárias sofreram grandes evoluções voltadas à segurança e velocidade diante as transações. A revista Mundo Estranho (2012), descreve o funcionamento de um caixa eletrônico onde o saque começa quando o cliente insere o cartão no leitor magnético. Na tarja contida no cartão é armazenado o número da conta e o da agência, com isto o leitor recebe estas informações e as valida para liberar o uso do caixa eletrônico, lembrando que esta liberação ocorre após a validação da senha do correntista. O correntista quando autenticado poderá fazer diversas operações que vão desde a consulta de saldo e saque até transferências e pagamentos.

Na Figura 1, um correntista efetuando uma transação em um caixa eletrônico por meio de um cartão.



Figura 1 - Transação em caixa eletrônico.

Fonte - Serviço Bancários (2010).

2.2. Cartões Magnéticos

Segundo a A3M (2014), os cartões magnéticos são cartões plásticos normais, nos quais é adicionada uma banda magnética no processo de fabricação. Os cartões juntamente com a tarja são lidos quando passados em uma cabeça de leitura magnética. É possível ler esses cartões todas as vezes que for preciso. O registro de dados sobre a tarja magnética utiliza a propriedade que tem certos materiais que se magnetizam de maneira duradoura sob a ação de um campo magnético. A tarja no verso de um cartão é composta de partículas magnéticas à base de ferro espalhadas por uma película semelhante a um filme. Os pequenos imãs, que compõem a tarja, são magnetizados e sua gravação é muito parecida com a de uma fita K7. Na Figura 2, um cartão magnético, sem a presença de um *chip*.



Figura 2 - Cartão Magnético.

Fonte - G1 Rio (2014).

2.3. Smart Cards

Para a ARISP (2014), *smart card* é um cartão criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor o certificado digital, que é um arquivo utilizado para comprovar sua identidade para outra pessoa ou outro computador, o que é considerado mais seguro que o cartão de tarja magnética. Teoricamente uma vez geradas essas chaves, elas estarão totalmente protegidas, não sendo possível exportá-las para outra mídia nem retirá-las do *smart card*.

Em reportagem divulgada no portal do Jornal Nacional (2010), para evitar fraudes, muitos bancos brasileiros implantaram o chip nos cartões. Segundo este jornal, o chip do cartão é de fato mais seguro, o problema está na tarja magnética, que têm informações que podem ser copiadas e utilizadas para gerar um cartão "clone". Na reportagem a Associação dos Cartões (ABECS) diz que os Estados Unidos e alguns países da América do Sul não adotaram o chip e por isso a tarja é mantida. Sem a tarja não seria possível viajar para algum desses países, e realizar compras nos mesmos, logo, a tarja se mantém por questões de compatibilidade.

2.4. Vulnerabilidade dos cartões e caixas eletrônicos

Pelos caixas eletrônicos é possível fazer pagamentos, aplicações e transferências sem a necessidade da presença de um funcionário do banco, sem enfrentar filas e ainda melhor, fora do expediente bancário, porém é um engano, acreditar que as operações sejam totalmente seguras conforme cita a revista Veja online (2001); apesar de toda tecnologia residida nos dispositivos de automação bancária, como os cartões e caixas eletrônicos, os jornais frequentemente noticiam fraudes envolvendo os mesmos.

Como exemplo houve uma reportagem exibida pelo portal G1 Distrito Federal (2014), em que um grupo fraudava cartões de crédito em Samambaia, Vicente Pires e Goiânia no estado de Goiás. Na reportagem a polícia diz que foram usados números de pelo menos 2 mil cartões, com média de compra de R\$ 1 mil por cartão. Com base nessa informação, é possível estimar que o grupo tenha causado um prejuízo de R\$ 2 milhões. Segundo a reportagem, os suspeitos conseguiam de 10 a 15 números de cartões por dia, que eram usados para comprar passagens aéreas, joias, eletrodomésticos e até ingressos para shows musicais.

Conforme o site Cidade Verde (2012), no Brasil, 33% dos consumidores já sofreram algum tipo de fraude envolvendo cartões, o que dá ao país a 7ª colocação em ranking de fraudes nesta categoria.

Para a FEBRABAN (2009), a segurança é uma preocupação central de seus bancos associados, tanto que o investimento anual em segurança é de cerca de R\$ 9,4 bilhões, três vezes superior ao valor do início da década. Parte deste investimento é direcionada aos caixas eletrônicos, equipamentos robustos, com elevado grau de resistência.

Este alto investimento visa evitar que criminosos apliquem fraudes, contudo estes sempre encontram novas possibilidades para ações criminosas as quais colocam em dúvida a segurança existente nos caixas eletrônicos e muitas vezes estas fraudes são aplicadas de forma grosseira, fazendo uso de dispositivos simples, como é mostrado a seguir na Figura 3.



Figura 3 - Dispositivos utilizados em clonagem de cartões.
Fonte - G1 Goiás (2013).

Apoiando-se no conceito de que criminosos sempre buscam novas formas para a realização de fraudes é notória a vulnerabilidade dos caixas eletrônicos quando analisados os sistemas operacionais destes dispositivos de automação bancária, pois segundo Gusmão (2014), por meio da revista Info, mostra que 95 % dos caixas eletrônicos do mundo ainda utilizam Windows XP, sendo que este sistema operacional não recebe mais suporte de atualizações da Microsoft, tornando-o suscetível a crackers, vírus e consequentemente expõe os consumidores ao risco de fraudes.

A seguir, algumas formas que os falsários utilizam para subtrair os dados de cartões, e posteriormente aplicar a fraude.

2.4.1. Fraude “Troca de Cartões”

Este golpe visa substituir o cartão do correntista por outro cartão e ao mesmo tempo obter as senhas digitadas pelo mesmo, conforme cita Cerigatto (2011). Tal golpe se dá quando um estelionatário oferece ajuda a uma pessoa que está passando por dificuldades diante a operação do caixa eletrônico e aproveita para “instruir” a vítima e ao mesmo tempo visualizar as senhas digitadas pela mesma. Diante desta fraude o criminoso retira rapidamente o cartão da vítima e o substitui por outro cartão da mesma agência. Futuramente o criminoso, em posse do cartão da vítima, realiza o roubo de identidade fazendo uso do cartão para compras, pois o mesmo possui um cartão original e as senhas da real correntista. Em geral esta fraude é descoberta quando a vítima retorna ao banco e tenta efetuar transações sem sucesso com o cartão que lhe fora entregue pelo criminoso.

2.4.2. Fraudes ocasionadas por descuidos do usuário

Segundo a FEBRABAN (2008), os bancos são responsáveis pela preservação da integridade, da legitimidade, da confiabilidade, da segurança e do sigilo das transações realizadas nos serviços que oferecem, mas sua ação protetora não consegue garantir isso nas ações e atitudes que dependem exclusivamente dos clientes.

Um problema muito comum acontece quando por ingenuidade, o usuário do caixa eletrônico anota a senha no próprio cartão, o que ocorre muitas vezes com idosos pela dificuldade de se memorizar a senha. Outra forma do usuário ter o cartão e a senha subtraída é por pessoas próximas, consideradas de “confiança”, que se aproveitam de uma oportunidade de descuido para agirem. Por isso a FEBRABAN orienta jamais fornecer senhas a terceiros, não anotar senhas em papéis, rascunhos ou no próprio cartão, caso contrário haverá a possibilidade de fraude.

2.4.3. Fraudes através dos *Credit Card Skimming* ou “chupa-cabras”

Conforme Rohr (2012), outra modalidade muito conhecida e que mais preocupa os brasileiros a tempos, é a utilização de um dispositivo conhecido vulgarmente como “chupa-cabra” ou em inglês “*Credit Card Skimming*”, que “clona” o cartão, subtraindo os dados nele contido e a senha do cliente. Este dispositivo é colocado discretamente nos caixas eletrônicos,

de forma que, o cliente ao utilizar o serviço, não o perceba. O cliente insere o cartão no “chupa-cabra” pensando ser realmente o verdadeiro dispositivo de leitura de cartões do caixa eletrônico, onde ocorre a clonagem. A polícia denomina de “cartãozeiros” os criminosos que aplicam este tipo de golpe.

Existem também quadrilhas que se especializam em roubar cartões entregues em domicílio. Conforme explica reportagem divulgada pela Veja online (2001), eles são clonados e depois enviados normalmente ao verdadeiro proprietário, que nem desconfia do problema até ver o próximo extrato. Nesse caso, é comum que os falsários telefonem dizendo serem funcionários do banco para confirmar a senha escolhida pela vítima.

A clonagem representa mais de 50% do total de fraudes praticadas com cartões. Ela acontece também em postos de gasolina e restaurantes. Quando o funcionário leva o cartão até a leitora e sem que o cliente perceba, o passa primeiro numa máquina portátil, que copia os dados de sua tarja magnética que posteriormente serão repassados para outro cartão. A seguir, na Figura 4, o equipamento de clonagem utilizado pelos golpistas.



Figura 4 - “chupa-cabra”.
Fonte - Monitor das fraudes (2014).

2.4.4. *Fraudes em Smart Cards*

O Jornal Estadão (2002), através de suas páginas, anunciou que os bancos Bradesco e Real estavam em fase de substituição da tarja magnética pelo *chip*, ou como descrito anteriormente, o *Smart Card* (Cartão Inteligente ou *chip*). Logo, no Brasil, a tecnologia está em uso a um pouco mais de 10 anos.

A substituição da tecnologia de tarja magnética, segundo o jornal Estadão (2002), veio na intenção de garantir aos clientes uma maior segurança nas operações eletrônicas e também agregar inúmeras funções em um único cartão tais como débito, crédito, vale alimentação e também evitar a clonagem da tarja magnética.

Tal afirmação hoje se encontra defasada, pois segundo o Portal G1 (2007), o *Smart Card*, que antes era considerado a prova de fraudes, já não é mais.

Informações do Departamento de Polícia Federal (2007) obtidas na operação denominada “Pen-Drive”, operação descrita no portal da Polícia Federal e relatada no Portal G1 (2007), reporta que um grupo de criminosos burlou a segurança existente nos cartões com chip, permitindo cloná-los. Para a Polícia Federal, esta foi à primeira ocorrência de fraude de *Smart Cards* no mundo. Ao todo, 11 mil pessoas de São Paulo e Curitiba tiveram seus cartões clonados.

A quadrilha contava com o apoio técnico, que segundo o jornal O Globo (2007), vinha de um engenheiro eletrônico, o qual fora contratado pelo chefe da quadrilha, Reinaldo Menezes do Sacramento, para o desenvolvimento do sistema de clonagem de cartões.

Segundo Zmoginski (2007), o engenheiro oferecia a tecnologia a grupos especializados na clonagem de cartões, já o restante dos criminosos subornava hotéis e postos de gasolina substituindo as máquinas de cartão por máquinas adulteradas, que não só armazenavam informações do cartão da vítima como também as senhas digitadas no pagamento. Após o suborno e instalação dos dispositivos, os criminosos retornavam aos locais onde estavam presentes as máquinas adulteradas e recolhiam os chips que armazenaram as informações das vítimas, realizavam a clonagem dos cartões com os dados armazenados nos chips e posteriormente utilizavam estes cartões clonados para compras no exterior.

Devido a esta insólita fraude, O Globo (2007) reporta que a operação contou com o apoio do serviço secreto americano que rastreou a ação dos criminosos no paraíso fiscal do Panamá. Para acompanhar a operação e buscar entender a tecnologia dos criminosos, vieram ao Brasil, representantes da empresa *Master Card* dos Estados Unidos.

2.5. Estatísticas sobre as fraudes

Em reportagem ao portal UOL realizada por Freitas (2013), Henrique Takaki, coordenador do Comitê de Segurança e Prevenção à Fraude da Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS), 85% das transações são feitas no Brasil com cartões com chip. Em outros países, como os Estados Unidos e os países da América

Latina, as máquinas que leem chip ainda são minoria, logo, pode ocorrer de a tarja magnética ser clonada e o cartão ser usado para compras lá fora e o pior, em moeda estrangeira.

Analizando os dados disponibilizados pelo INSPER e CPP (2013), podemos observar que crimes de estelionato tiveram um aumento significativo, como no caso de fraudes em cartões de crédito, que apresentaram um aumento de 327,5% de 2003 a 2013, isso somente no estado de São Paulo. Aliás, se for feita uma comparação com outros tipos de fraudes, foi a que mais evoluiu. Conforme demonstra a Tabela 1.

Tabela 1 - Comparação de fraudes em cartões em relação a outras fraudes.

<u>Estelionato</u>	<u>Parcela de entrevistados vitimizados</u>				
	<u>2003</u>	<u>2008</u>	<u>2013</u>	<u>Var. 2008/13</u>	<u>Var. 2003/13</u>
Notas de dinheiro falso	15,4%	12,6%	8,0%	<u>-36,6%</u>	<u>-47,9%</u>
Fraude contra o seu cartão de crédito	1,4%	2,7%	5,9%	<u>118,5%</u>	<u>327,5%</u>
Cheque que não pode ser descontado	7,4%	4,6%	3,7%	<u>-20,6%</u>	<u>-50,1%</u>
Pagou por algum produto que não foi entregue	1,3%	1,1%	1,8%	<u>64,9%</u>	<u>36,6%</u>
Linha telefônica residencial violada ou desviada	2,2%	2,7%	1,7%	<u>-37,7%</u>	-23,4%
Vítima de fraude em algum investimento que realizou	0,9%	0,8%	0,7%	-10,3%	-22,2%
Celular clonado	0,7%	1,1%	0,7%	<u>-38,0%</u>	1,5%
Fraude de documentos pessoais	0,7%	0,7%	0,6%	<u>-18,9%</u>	-9,1%
Comprou apólices falsas de algum tipo de seguro ou plano de previdência	0,2%	0,2%	0,1%	-23,5%	-40,9%
Títulos falsos de propriedades de imóveis	0,1%	0,1%	0,1%	-30,0%	-12,5%
Problema com site de compra			1,6%		
Fraude bancária na internet			0,5%		

Fonte - CPP, INSPER (2013).

Com base no elevado índice de clonagem descrito anteriormente existe a necessidade constante de investimento em segurança tecnológica nos bancos, pois diante uma transação bancária o caixa não consegue identificar a autenticidade física de um real correntista, exceto com o uso da biometria. Desta forma, a não autenticação biométrica, permite que criminosos sempre busquem novas formas para burlar os sistemas existentes nos caixas eletrônicos.

2.6. Bancos e o investimento em segurança biométrica

Devido aos altos índices de fraudes e os elevados valores em prejuízos citados anteriormente, os bancos investem alto em segurança. Através dos investimentos as instituições bancárias buscam soluções tecnológicas para evitar ou reduzir fraudes. Alguns bancos já adotam a biometria através da impressão digital para a autenticação de um correntista em um caixa eletrônico, uma destas instituições é o Itaú. O uso da impressão digital, segundo nota do próprio banco Itaú (2012), aumenta a segurança e velocidade das transações bancárias no caixa eletrônico, pois torna desnecessário o uso do cartão e senhas para saques de valores baixos, ou seja, somente com a impressão digital já é possível realizar operações nos caixas eletrônicos, como mostrado na Figura 5, onde uma correntista está fazendo uso do sistema biométrico no caixa eletrônico.



Figura 5 - Exemplo do uso de um sistema biométrico.

Fonte - Nocelli (2014).

A biometria utilizada nos bancos visa detectar além da impressão digital os padrões da circulação sanguínea existentes no dedo do possível correntista e desta forma garantir a autenticidade do mesmo.

Nos próximos capítulos será explanado a respeito das técnicas e conceitos da biometria facial no intuito de possibilitar o entendimento da mesma, sendo que esta será a ferramenta proposta para o aumento da segurança nos caixas eletrônicos.

3. IDENTIFICAÇÃO BIOMÉTRICA

Segundo Cabral (2014), a biometria faz uso das características biológicas de uma pessoa a fim de promover mecanismos únicos de identificação. Essa identificação pode ser realizada, por exemplo, através de elementos corporais que não são iguais, ou seja, elementos que contém diferenças particulares. Bonato e Neto (2010) complementam afirmando que biometria é a ciência que procura identificar indivíduos baseando-se em características particulares. Essas características podem ser de caráter fisiológico, que estão relacionadas com a forma do corpo. Os exemplos incluem, mas não estão limitados a impressão digital, reconhecimento facial, geometria da mão e de biometria ocular compreendida entre reconhecimento da íris e da retina. Também podendo ser classificada como biometria comportamental, que está relacionada ao comportamento de uma pessoa, característica que pode ser implementada através da verificação de assinatura, dinâmica de digitação e voz. Seu principal papel nos dias atuais é controlar o acesso de pessoas a um determinado local que exige um alto nível de segurança.

Para Slaibi Conti (2012), cada indivíduo possui características únicas capaz de diferenciá-lo de outros seres humanos, mesmo que sejam gêmeos vitelinos, idênticos em sua forma física. A explicação simples parte do fato de que estas características como: digitais, pregas de flexão, dobras e cristais que são ondulações palmares (mãos) e plantares (pés), são heranças determinadas por fatores genéticos e ambientais (intra e extra-uterino).

Conforme específica a CBA (2014), todos os produtos biométricos operam basicamente de forma similar. Primeiro, é extraída uma amostra da característica biométrica durante um processo de cadastramento. Durante o cadastro, alguns sistemas biométricos requerem que um número de amostras seja dado para construir-se um perfil da característica biométrica. Atributos únicos são então obtidos e convertidos pelo sistema em um código matemático. Essa amostra é então armazenada como o modelo biométrico daquela pessoa. O modelo pode residir em um sistema biométrico ou em qualquer outra forma de memória de armazenamento, como um banco de dados do computador, um cartão inteligente ou um código de barras.

3.1. Aplicação da Biometria

Segundo o TSE (2013), biometria pode ser utilizada em vários lugares para melhorar a segurança ou conveniência dos cidadãos. No Brasil, a emissão de passaporte, de carteiras de

identidade e o cadastro das Polícias Civil e Federal contam com sistemas biométricos. Além disso, muitas empresas adotam tais sistemas para acesso às suas instalações ou utilização de seus serviços. É o caso de algumas academias de ginástica que usam leitura da impressão digital para controlar o acesso dos seus frequentadores.

Para Silva et. al. (2007), com as soluções de biometria, o que muda é o rigor da informação utilizada para sermos autenticados e a verificação da mesma. As soluções de biometria aumentam a segurança porque comparam quase imediatamente as características únicas de um indivíduo com as mesmas que estão armazenadas numa base de dados. Além disso, como envolvem características biométricas (intrínsecas ao indivíduo), não existe o risco de perder os elementos identificadores ou de nos esquecermos deles (exceto nos casos de acidentes com consequências físicas e/ou comportamentais).

3.2. Requisitos da Biometria

Conforme citado por Jain et. al (1997), no artigo “Um sistema de autenticação de identidade usando impressões digitais” (*An Identity Authentication System Using Finger prints*) uma característica fisiológica pode ser usada para identificação biométrica desde que preencha os seguintes requisitos.

- **Universalidade:** Todas as pessoas devem possuir aquela característica.
- **Singularidade:** Duas ou mais pessoas não podem possuir características iguais ou semelhantes a ponto de confundir o sistema.
- **Permanência:** A característica não pode sofrer variações com o tempo.
- **Colecionabilidade:** Indica que a característica possa ser medida quantitativamente.
- **Desempenho:** Representa como já citado, à precisão de identificação diante a necessidade de superar taxas de falhas e alcançar uma identificação aceitável.
- **Aceitabilidade:** Demonstra a que ponto as pessoas estão dispostas a aceitarem a técnica biométrica.
- **Evasão:** Indica o nível de possibilidades para que o sistema seja fraudado.

Na Tabela 2 é possível visualizar um comparativo entre os tipos de biometria.

Tabela 2 - Comparação entre os tipos de biometria.

Biometrias	Universalidade	Singularidade	Permanência	Colecionabilidade	Desempenho	Aceitabilidade	Dificuldade de falsificação
Face	Alto	Baixo	Médio	Alto	Baixo	Baixo	Baixo
Impressão Digital	Médio	Alto	Alto	Médio	Alto	Médio	Alto
Geometria da Mão	Médio	Médio	Médio	Alto	Médio	Médio	Médio
Veias da Mão	Médio	Médio	Médio	Médio	Médio	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Retina	Alto	Alto	Médio	Baixo	Alto	Baixo	Alto
Assinatura	Baixo	Baixo	Baixo	Alto	Baixo	Alto	Baixo
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

Fonte - Jain et al (1997). Adaptada.

3.3. Tipos de Biometria

Características biométricas, para Ibiométrica (2014), podem ser divididas em duas classes principais: Físicas e Comportamentais.

3.3.1. Biometria Fisiológica

Como descrito anteriormente, na primeira seção deste capítulo, a biometria fisiológica está relacionada com as formas do corpo humano. A seguir algumas formas de identificação biométrica, classificadas como fisiológicas.

- Impressão digital**

Para Ibiométrica (2014), os padrões de cristas e vales de fricção dos dedos são únicos de cada indivíduo. As impressões digitais são únicas para cada dedo de uma pessoa, incluindo os gêmeos idênticos. Umas das tecnologias biométricas mais comercialmente disponível são

os dispositivos de reconhecimento de impressões digitais para acesso de desktop e laptop, que são agora amplamente disponíveis a um custo baixo. Com esses dispositivos, os usuários não precisam digitar senhas, em vez disso, apenas um toque oferece acesso instantâneo.

Conforme informações da CBA (2014), as biometrias de digitais são amplamente conhecidas como um método preciso de identificação e verificação biométrica. Elas podem ser definidas como os contornos das linhas papilares ou bifurcações (ramificações das linhas papilares). Outros sistemas de impressões digitais analisam os pequenos poros no dedo que, assim como as minúcias, são posicionados de forma única para diferenciar uma pessoa de outra. A densidade da imagem digital ou a distância entre as linhas papilares também podem ser analisadas. Os contornos de uma digital são exemplificados na Figura 6 a seguir.



Figura 6 - Pontos identificadores das digitais
Fonte - Bonato, Neto (2010)

Certas condições podem afetar as impressões de diferentes indivíduos. Por exemplo, sujeira, dedos secos ou rachados podem reduzir a qualidade da captura da imagem. Idade, sexo e etnia também podem impactar a qualidade das imagens digitais. A forma como um usuário interage com um scanner de digitais é outra consideração importante. Pressão muito forte na superfície do scanner, por exemplo, pode distorcer uma imagem, tanto que alguns scanners são ergonomicamente desenhados para otimizar o processo de captura de impressões digitais.

• Geometria da Mão

Conforme afirma Amorim (2005), sua aplicação se baseia na premissa básica que virtualmente não existem duas pessoas com mãos idênticas. Por meios de imagens capturadas,

definições de alguns pontos e cálculos, são definidas as dimensões de determinados pontos da mão que serão usados pelo sistema para permitir ou restringir o acesso de um usuário.

Segundo a CBA (2014), a biometria de geometria da mão tira uma imagem tridimensional da mão e mede o seu tamanho e o comprimento dos dedos e das articulações. É um dos preferidos da indústria e tem sido utilizado por muitos anos, predominantemente para aplicações de controle de acesso. Seu uso é conveniente e a vantagem primordial é a grande quantidade de usuários que podem ser processados rapidamente. Apesar deste método processar vários usuários rapidamente, Amorim (2005) considera a geometria da mão um método pouco seguro, o fator negativo deve-se ao fato de que a geometria da mão sofre alterações durante a vida de um ser humano (a idade, perda ou ganho de peso, etc.).

• Biometria Ocular

Para Garcia (2009), a estrutura da biometria ocular, se divide em biometria da íris e biometria da retina.

a) Identificação pela Íris - Segundo a Ibiométrica (2014), a íris é o anel colorido que circunda a pupila do olho. Toda íris possui uma estrutura única, caracterizando um padrão complexo. Pode ser uma combinação de características específicas como coroa, glândula, filamentos, sardas, sulcos radiais e estriamentos. É conhecido que uma duplicação artificial da íris é virtualmente impossível devido às suas propriedades únicas. A íris é estritamente ligada ao cérebro humano e uma das primeiras partes a se desintegrar após a morte. É portanto muito improvável que uma íris artificial possa ser recriada ou que uma íris morta possa ser usada para fraudar a passagem no sistema biométrico.

Conforme destaca a CBA (2014), os padrões da íris são obtidos através de um vídeo baseado em sistema de aquisição de imagem. Os dispositivos de varredura da íris têm sido utilizados em aplicações de autenticação pessoal por vários anos. Os sistemas baseados no reconhecimento de íris diminuíram substancialmente de preço e esta tendência deverá continuar. Os sistemas atuais podem ser usados, mesmo na presença de óculos e lentes de contato. A tecnologia não é intrusiva, pois não requer contato físico com um scanner. O reconhecimento da íris foi demonstrado para trabalhar com pessoas de diferentes etnias e nacionalidades.

Na Figura 7 um exemplo de uma íris.

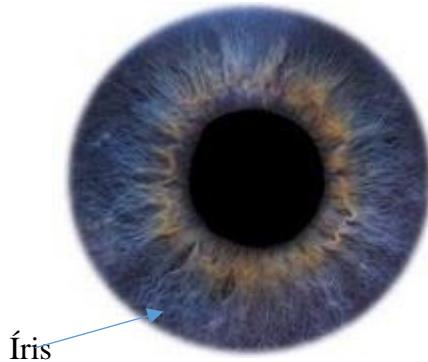


Figura 7 - Íris
Fonte - Acesso e Ponto (2014).

Para Garcia (2009), a biometria da íris é um método de identificação muito confiável, pois apresenta uma baixa taxa de falsa rejeição (2,5%) e também baixa taxa de falsa aceitação (0,0001%). Sua taxa de erro é de 1 em 1,2 milhões. Além do mais a íris apresenta uma estrutura estável ao longo da vida, pois está protegida dentro de um órgão sem contato com o mundo externo.

b) Identificação pela Retina - Segundo a Ibiométrica (2014), a retina humana é composta por um tecido fino de células neurais que está localizado na porção posterior do olho como é demonstrado na Figura 8. Devido à complexa estrutura dos vasos capilares que suprem a retina com sangue, a retina de cada pessoa é única. A rede de vasos sanguíneos na retina é tão complexa que mesmo gêmeos idênticos não compartilham um padrão semelhante. Embora os padrões de retina possam ser alterados nos casos de diabetes, glaucoma, doenças degenerativas da retina ou cataratas, como afirma Amorim (2009), a retina geralmente permanece inalterada desde o nascimento até a morte. Devido à sua natureza única e imutável, a retina parece ser a eleição dos advogados por serem as mais precisas e fiáveis estruturas biométricas.

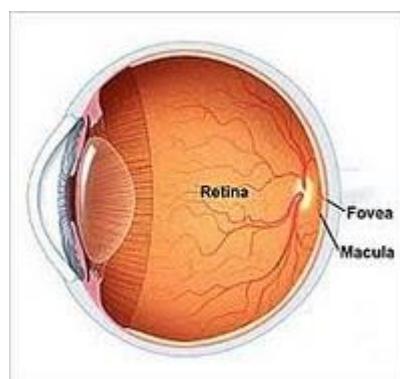


Figura 8 - Exemplo Retina
Fonte - Acesso e Ponto (2014)

- **Reconhecimento Facial**

Segundo Beymer e Poggio (1995), o ser humano desenvolve a capacidade de reconhecer as pessoas pela face muito cedo. Crianças com poucos meses de vida já são capazes de reconhecerem as pessoas mais próximas. Esta capacidade é adquirida pelo cérebro humano na medida em que crescemos, tornando-se uma ferramenta de reconhecimento que quase todos os seres humanos possuem. Mesmo com o passar dos tempos, ou com muitas transformações na face das pessoas conhecidas, mesmo quando por necessidades passam a usar óculos, deixem a barba crescer ou um corte de cabelo diferente, o reconhecimento acontece normalmente. Já num sistema automático de reconhecimento de faces deve-se considerar que estes fatores, ou até mesmo a expressão facial do momento da leitura, podem afetar diretamente o reconhecimento.

Por isso, como afirma a CBA (2014), identificar um indivíduo através da análise da face é um processo complexo que normalmente requer artifícios inteligentes sofisticados e técnicas de aprendizagem computacional (*machine learning techniques*). A aprendizagem computacional é importante para a adaptação a essas mudanças e para comparar precisamente os novos exemplos com os modelos previamente armazenados.

3.3.2. Biometria Comportamental

Esta classificação biométrica está relacionada ao comportamento de uma pessoa. Característica implementada usando a biometria com a verificação de assinatura, reconhecimento por voz, além de outros.

- **Sistemas de Reconhecimento por Voz**

Conforme explica Amorim (2005), a identificação de uma pessoa feita através de sua voz é extremamente fácil de usar e é considerada não intrusiva pelos usuários. Apesar da facilidade de manipular os dados deste tipo de identificação, ele não é considerado confiável. O programa de identificação faz uma análise dos padrões harmônicos e não uma simples comparação entre reproduções de uma mesma fala.

Segundo Otaviano (2005), assim como acontece em impressão digital, a identificação de uma pessoa pela voz, depende diretamente das características particulares a cada pessoa. No caso da voz, vários coeficientes podem ser extraídos.

Uma vez que padrões de fala se formam através da combinação de fatores físicos e comportamentais, existem problemas como as condições do ambiente onde se encontram os

sensores de captação da voz a ser identificada, uma vez que é difícil filtrar o ruído de fundo; a variação da voz também depende das condições físicas do usuário, como gripes e resfriados e ainda estados emocionais como o estresse, e duplicação através de um gravador.

Segundo a Ibiométrica (2014), a voz também pode ser classificada como uma característica fisiológica, porque cada pessoa tem um tom diferente, mas o reconhecimento de voz é principalmente baseado no estudo da forma como uma pessoa fala, comumente classificadas como comportamentais.

- **Biometria de Assinatura**

Segundo a Ibiométrica (2014), o reconhecimento biométrico de assinatura irá medir e analisar a atividade física da assinatura, como a ordem da escrita, a pressão aplicada e da velocidade inserida para a confecção da mesma. Alguns sistemas também podem comparar imagens visuais de assinaturas, mas o núcleo de um sistema de assinatura biométrica é comportamental, ou seja, como é assinado e não a imagem da assinatura. Portanto conforme explica a CBA (2014), mesmo que uma assinatura seja copiada, um impostor precisará saber a dinâmica da assinatura. Isso torna a falsificação muito difícil.

3.4. Modos de operação para biometria.

Segundo o TSE (2013), na biometria, o procedimento de reconhecer um usuário ocorre de duas formas distintas. Todo sistema biométrico é preparado para verificar ou identificar uma pessoa que foi previamente cadastrada.

- **Verificação (“Um-para-Um” ou 1:1)**

Os sistemas biométricos de verificação apenas comparam dois modelos e determina se os dois *modelos* são, de fato, da mesma pessoa. Normalmente um dos *modelos* está gravado em banco de dados enquanto o outro é adquirido ao vivo.

- **Identificação (“Um-para-Muitos” ou 1:N)**

Os sistemas biométricos de identificação comparam um modelo a todo o banco de dados e retornam a identidade da pessoa, caso a mesma tenha sido encontrada no banco de dados.

- **Comparação da Verificação (1:1) em relação a Identificação (1:N)**

A verificação (1:1) é um processo muito mais rápido em relação a identificação quando o número de usuários ultrapassa de 5000. Outra vantagem, é que em grande quantidade de usuários a verificação acaba se tornando mais segura.

3.5. Desempenho dos sistemas biométricos

Para aperfeiçoar os sistemas biométricos várias técnicas e algoritmos são empregados, contudo a assertividade da biometria pode ser influenciada por diversos fatores. Imagens de características biométricas de um mesmo indivíduo podem, quando comparadas, não serem exatamente iguais. Jain et. al (2004) citam que ocorrem variações na imagem tornando-a imperfeita, tais como alterações nas características fisiológicas ou comportamentais do usuário, que no caso da biometria facial podem ser exemplificadas por cicatrizes na face, hematomas, uso de óculos, barba e condições ambientais (umidade e temperatura).

Na Figura 9 estão presentes as etapas de obtenção de modelos e comparação dos mesmos para possibilitar o entendimento da mecânica dos sistemas biométricos e da extração dos índices de assertividade dos mesmos.

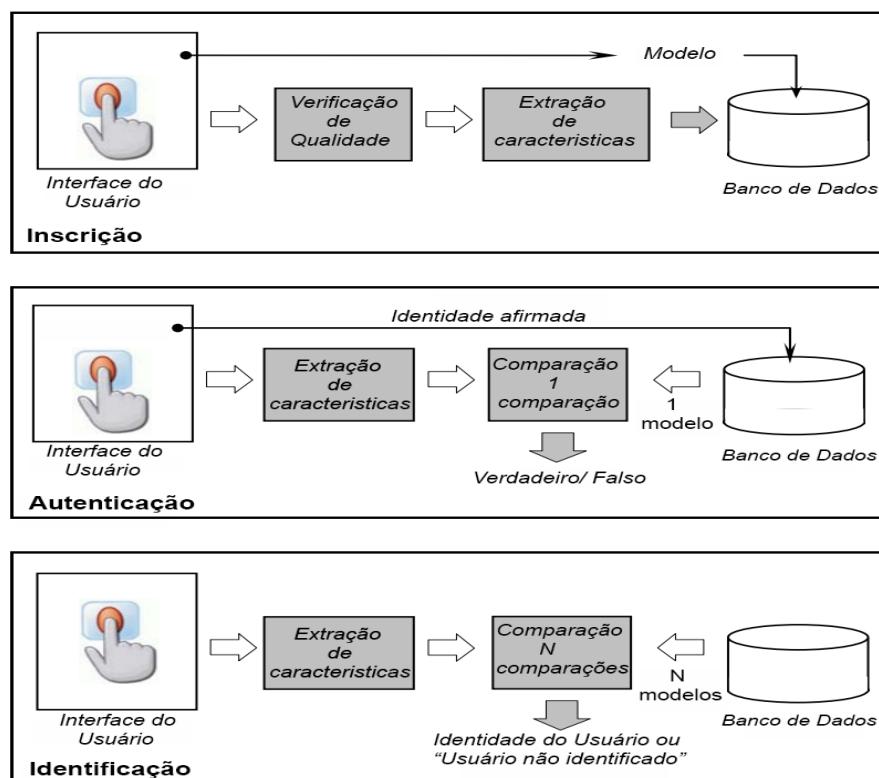


Figura 9 - Principais operações biométricas: autenticação (verificação) e identificação (reconhecimento).
Fonte - Jain et. al (2004). Adaptada.

A variabilidade intraclasse e similaridade interclasse de uma amostra também afetam no processo de comparação de imagens, ou seja, para a variabilidade intraclasse várias amostras de um mesmo indivíduo, obtidas diante uma autenticação (comparação um-para-um), podem apresentar diferenças significativas quando comparadas as amostras obtidas

diante o processo de inscrição (cadastramento dos modelos na base de dados) e para a similaridade interclasse é quando características de classes diferentes, ou melhor, de indivíduos diferentes, se apresentam de forma semelhante diante a comparação.

Conforme citado por Jain et al (2004), a resposta de um sistema de correspondência biométrica é a pontuação $S(Xq, Xi)$, normalmente um número único, que quantifica a similaridade entre a entrada e o modelo da base de dados (Xq e Xi respectivamente); para um melhor entendimento Xq corresponderá as imagens de entrada do sistema, que são as imagens que estão sendo obtidas para um processamento com Xi ; sendo que este último corresponde as imagens já cadastradas no banco de dados através do processo de inscrição presente na Figura 9. Quanto maior a pontuação de S , maior é a certeza de que as medidas biométricas de entrada e banco de dados sejam provenientes da mesma pessoa.

Para a avaliação do percentual de assertividade e falhas de um sistema biométrico faz-se uso de índices específicos, que são:

- Taxa de Falsos Positivos (TFP) também nomeada de *False Accept Rate* (FAR), que representa a falsa aceitação de um impostor como genuíno. Tal taxa é calculada pela seguinte equação.

$$TFP = \frac{\text{número de falsas aceitações}}{\text{número de tentativas de impostores}}$$

- Taxa de Falsos Negativos (TFN) ou *False Reject Rate* (FRR), que representa a falsa rejeição de um indivíduo autêntico ou genuíno como se fosse um impostor. Esta taxa é calculada pela seguinte equação.

$$TFN = \frac{\text{número de falsas rejeições}}{\text{número de tentativas de genuínos}}$$

Os sistemas biométricos tem sua principal funcionalidade determinada por um limiar (*threshold*), ou seja, se um número T de amostras gerarem escóres de similaridade maior ou igual a T são classificadas como amostras de uma mesma pessoa, caso contrário serão amostras de diferentes indivíduos. A distribuição das pontuações geradas a partir dos pares de amostra de uma mesma pessoa é chamada de genuína, já a distribuição de amostras de diferentes pessoas é denominada impostora.

Na Figura 10 é possível visualizar um modelo fictício das taxas de erro onde tanto TFP quanto TFN são funções do sistema de limiar t .

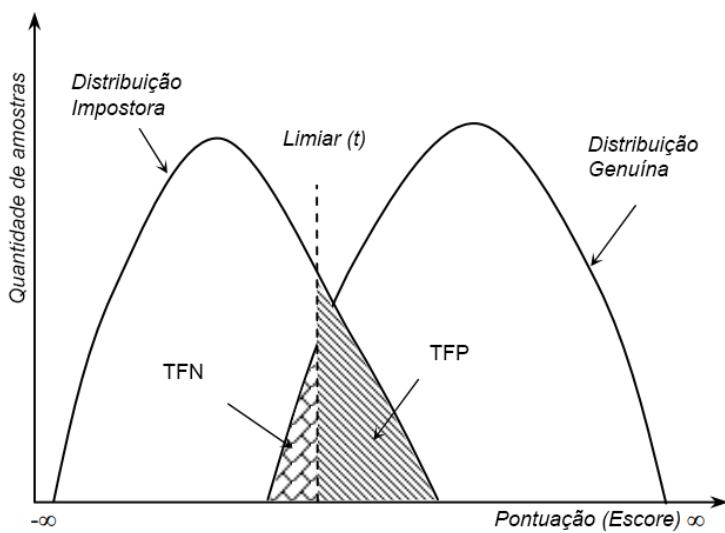


Figura 10 - Distribuição fictícia de falsos positivos e falsos negativos estabelecidos através de um limiar.

Fonte - Jain et al (2004). Adaptada.

Se t for alocado mais para a esquerda o sistema se tornará mais tolerante, contudo ocorrerá um aumento da TFP e caso t seja deslocado para a direita em busca de segurança, terá como consequência o aumento da TFN. Em outras palavras se o limiar for direcionado para a direita irá ocorrer maiores falhas diante da recusa de indivíduos genuínos (falso negativo) e quando o limiar for direcionado para a esquerda ocorrerá uma maior aceitação de indivíduos impostores como genuínos (falso positivo). Na Figura 10 é possível ver claramente este modelo e as possibilidades de deslocamento do limiar t .

Para Jain et al (2004), os erros diante a captura de imagens (*Failure To Capture* - FTC) e cadastro das mesmas (*Failure To Enroll* - FTE) também são fatores que influenciam no desempenho dos sistemas biométricos.

4. PROCESSAMENTO DE IMAGENS E VISÃO COMPUTACIONAL

Antes de qualquer entendimento dos conceitos específicos do reconhecimento facial será feita uma abordagem de alguns princípios de processamento de imagens e da visão computacional no intuito de familiarizar a leitura no entendimento desta área. Muitas vezes o entendimento da biometria facial, quando adquirida por um leigo, tende a ser mais oneroso, pois o mesmo não tem as bases e conceitos que definam a origem de todo o processo de reconhecimento facial e de que forma os algoritmos são executados a ponto de detectar regiões faciais e correspondências entre faces.

Neste capítulo será efetuada uma abordagem de simples algoritmos executados em uma imagem a ponto de alterá-la em seus aspectos visuais. Alguns conceitos mais aprofundados não serão abordados visando apenas familiarizar as bases do processamento de imagem e visão computacional.

Para Silva (2001) o principal objetivo do processamento de imagens é fornecer subsídios para auxiliar na extração e identificação de informações contidas em imagens, para futura interpretação. Com base neste conceito, sistemas dedicados de computação realizam atividades de análise e manipulação de imagens brutas, que são as imagens não processadas para realçar suas informações.

A informação de interesse é caracterizada com base nos objetos ou padrões que compõem a imagem, logo, a extração de informações de imagens envolve o reconhecimento de objetos ou padrões com base na capacidade cognitiva do interprete.

O sistema visual humano possui grande capacidade para reconhecer padrões, contudo, não é capaz de processar um grande número de informações presentes em uma imagem. Informações distorcidas através do processo de aquisição do olho humano podem limitar ainda mais esta capacidade humana, com isto surgiu o processamento de imagens, visando quebrar barreiras visuais do olho humano, permitindo facilitar os processos de extração de características (informações) em imagens.

4.1. O que é uma imagem a nível computacional?

Se aplicarmos um zoom em uma imagem digital, o qual pode ser feito por um editor de imagens, será possível visualizarmos esta imagem como se a mesma estivesse sendo dividida por uma grade a qual pode ser facilmente associada a um desenho sobre um papel quadriculado. Cada bloco ou quadrado desta grade é denominado pixel. Para Martins (2014),

o pixel (px), acrônimo de *Picture Element*, é o menor elemento de uma imagem digital. A junção de todo o aglomerado de pixels de uma imagem pode ser representada através de uma matriz, logo, uma imagem é composta de linhas e colunas onde o total de linhas determina a altura e o total de colunas determina a largura. Na Figura 11 as dimensões de largura e altura de uma imagem.



Figura 11 – Exemplo de dimensões de uma imagem.

O processamento de imagem, quando efetuado, realiza iterações nesta matriz de pixels através de laços de iteração (*for*, *foreach*, *while* e *do while*) presentes na linguagem de programação que está sendo utilizada.

Na Figura 12 é exemplificada a ampliação de uma região de interesse em uma imagem digital. Tal região recebeu um zoom, ou seja, foi ampliada a ponto de exibir a grade de pixels da imagem.



Figura 12 - Área da imagem com uma região de interesse ampliada.

Na área de processamento de imagens a região de interesse ou ROI (*Region of Interest*) é uma área da imagem digital a qual foi selecionada para ser processada. Para o processamento de imagem que envolve o reconhecimento facial a região de interesse é a face e quaisquer pontos ou objetos que não representem a face devem ser desconsiderados.

4.2. Processamento de imagem

Alguns elementos compõem um sistema de processamento de imagem com o objetivo de realizar operações de processamento, que segundo Gonzalez e Woods (1992), estes elementos são.

Aquisição de imagem - Dois elementos são necessários para a aquisição de imagens. O primeiro é um dispositivo físico sensível a uma banda do espectro de energia eletromagnética (ultravioleta, raios X, visível ou banda infravermelha) e que produza um sinal elétrico de saída proporcional a um nível de energia perceptível. O segundo, chamado digitalizador, é um dispositivo para conversão da saída elétrica de um dispositivo de sensoriamento físico para o formato digital. Em outras palavras é o ato de se adquirir uma imagem real por meio de um dispositivo (hardware) para uso em futuro processamento.

Armazenamento - Para que uma imagem seja persistida para futuro processamento computacional é necessário o armazenamento digital da mesma. Tal armazenamento digital é medido em byte (oito bits), *Kilobytes* (mil bytes), *Megabytes* (um milhão de bytes), *Gigabytes* (um bilhão de bytes), e *Terabytes* (um trilhão de bytes). A armazenagem é classificada em três principais categorias a seguir descritas.

- Armazenamento por curto tempo – O armazenamento por curto tempo é realizado somente durante o processamento e faz uso da memória computacional.
- Armazenamento “On-line” – Possibilita acesso rápido e faz, em geral, uso de discos rígidos para armazenamento. Um fato que caracteriza o armazenamento “on-line” é o frequente acesso a dados.
- Armazenamento em arquivo digital – É caracterizado pela necessidade de armazenamento massivo, mas sem necessidade de acesso frequente a tais arquivos de imagens. Também faz, em geral, uso de discos rígidos, assim como o armazenamento “on-line”, consequentemente tende a ter acesso rápido.

Processamento - Processamento de imagem digital envolve procedimentos que são geralmente representados em forma algorítmica. Assim, com exceção da aquisição e exibição de imagens, o processamento de imagem é realizado via software. O único motivo para hardware especializado em processamento de imagens vem da necessidade de se adquirir maior velocidade no processamento ou da necessidade de aplicações vencerem limitações de luminosidade. O processamento de imagem é caracterizado por soluções específicas. Desse modo, técnicas que funcionam bem em uma área podem não ser satisfatórias em outra área.

Comunicação - envolve a comunicação entre sistemas de processamento de imagem e comunicação remota de um ponto a outro, em conexão com a transmissão de dados de imagens. Pode ser representada pela comunicação de uma câmera IP com um servidor que processa faces e tenta detectar possíveis criminosos.

Exibição - Monitores de TV, monocromáticos e coloridos, são os principais dispositivos de exibição usados em processamento de imagem. Tais monitores são conectados a um computador hospedeiro que fornece como saída imagens digitais.

4.3. Limiarização

Segundo Mello (2014), a limiarização consiste na conversão de uma imagem para dois tons a partir de um dado ponto de corte denominado limiar, o qual em inglês é *threshold*. Na Figura 13, um algoritmo de recorte, o qual irá definir, através de um *threshold*, baseado em valores de histograma, como uma imagem será convertida em dois tons e quais tons irão prevalecer na imagem. No algoritmo a seguir dado como exemplo, o ponto de corte deve ser menor ou igual a 127. Caso satisfaça a condição a cor definida será preto, caso contrário a cor será branco

Se cor (i) ≤ 127

Então cor (i) = Preto

Senão cor (i) = Branco

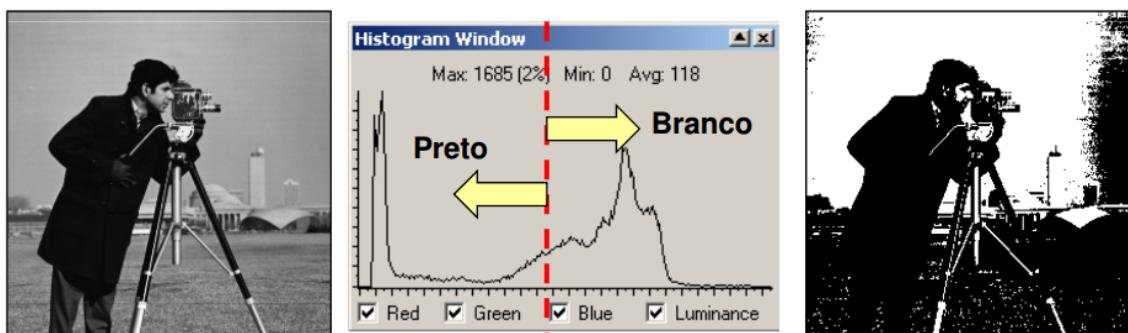


Figura 13 - Valor de Corte = 127
Fonte - Mello (2014).

4.4. Histogramas

Segundo Nemes (2011), a função principal dos histogramas é mostrar através de um gráfico qual é a situação real da imagem, e não o que está se enxergando. O histograma é dividido em regiões. O lado esquerdo é a região que concentra os tons escuros da imagem, o meio

mostra os tons médios e no lado direito ficam os tons mais claros. É como uma escala que vai do preto ao branco, partindo da esquerda até a direita.

Conforme Silva (2001, *apud* CEPSRM, 2014), em processamento de imagens, utiliza-se tons de cinza (*digital numbers* ou DN's) atribuídos aos pixels de uma imagem. Essa é uma das formas mais comuns de se demonstrar a distribuição dos DN's de uma imagem, e possivelmente a mais útil em processamento digital de imagens. Ele fornece a informação sobre quantos pixels na imagem possuem cada valor possível de DN (que, no caso das imagens de 8 bits, variam de 0 a 255) ou, de forma equivalente, qual a proporção da imagem que corresponde a cada valor de DN. Outro ponto importante com relação a histogramas é que eles representam dados digitais, também chamados de discretos. Assim sendo, a distribuição de intensidades é representada por colunas discretas, que não podem ser divididas ou "quebradas", correspondentes a números inteiros. Esse conceito assume importância ao se tratar de realce de contraste em imagens.

4.5. Equalização de Histogramas

Em processamento de imagens, após a aquisição das mesmas, pode haver a necessidade de ajustes, de forma a compatibilizar algumas distorções que podem ocorrer durante a etapa de aquisição das imagens, principalmente por parte de diferenças de iluminação de ambiente e dos dispositivos de captura, o que poderia comprometer futuramente o processo de reconhecimento das texturas durante as etapas de reconhecimento e comparação das características das imagens.

Conforme artigo publicado pelo Departamento de Informática da Universidade Federal do Pernambuco (2014), equalizar o histograma significa obter a máxima variância do histograma de uma imagem, obtendo assim uma imagem com o melhor contraste. O contraste é uma medida qualitativa e que está relacionada com a distribuição dos tons de cinza em uma imagem. Para equalização do histograma, utilizam-se três tipos de técnicas: equalização global, equalização regional por blocos e equalização regional pontual. A equalização global do histograma consiste em executar um processo de reorganização dos tons de cinza presentes na imagem, redistribuindo-os de forma que estes fiquem distribuídos de forma homogênea por toda a faixa de tons de cinza disponível (mais próximo de um histograma ideal com igual número de pixels para cada tom).

4.6. Visão Computacional

Conforme Milano e Honorato (2014), visão computacional é a ciência responsável pela visão de uma máquina, pela forma como um computador enxerga o meio à sua volta, extraíndo informações a partir de imagens capturadas por câmeras de vídeo, sensores, scanners, entre outros dispositivos. Estas informações permitem reconhecer, manipular e pensar sobre os objetos que compõem uma imagem. As aplicações que utilizam visão computacional são para resolver problemas particulares de forma específica. Para Milano e Honorato (2014), estes sistemas são conhecidos como sistemas especialistas, que necessitam de uma base de conhecimento para a solução de um determinado problema. Dessa forma, não existe um modelo padrão bem definido. Porém, basicamente todos os sistemas de visão computacional envolvem reconhecimento de objetos em imagens e transformações destes objetos em informações que serão processadas e utilizadas por algum sistema especialista.

5. RECONHECIMENTO FACIAL

O reconhecimento facial é citado por Li e Jain (2005) como uma tarefa empregada pelos seres humanos sem esforço algum e realizada de forma rotineira. Tal habilidade, devido a sua capacidade de distinguir indivíduos, abre portas para um vasto cenário de possibilidades. Com a redução dos custos voltados ao poder de processamento dos computadores o reconhecimento facial está se tornando foco de interesse no que diz respeito a processamento automático de imagens digitais e vídeos, devido a seu uso quando somado a diversas aplicações, às quais podem ser exemplificadas por sistemas de vigilância, interações humano-computador e investigações forenses.

As pesquisas voltadas para o reconhecimento facial não estão voltadas para a solução de problemas e sim, pelas aplicações práticas nas quais é necessária a identificação humana, ou seja, o reconhecimento facial não evolui para solucionar um problema em específico e sim para contribuir com diversas aplicações nas quais é necessária a identificação de uma face.

As características do reconhecimento facial o definem como vantajoso quando comparado a outras tecnologias, pois é natural e não intrusivo, ou seja, é capaz de identificar um indivíduo sem a sua colaboração de forma rápida e sem incômodo.

5.1. Sistema de reconhecimento facial

De acordo com Diniz et al. (2013), um sistema de reconhecimento facial, assim como representado na Figura 14, possui algumas etapas para seu correto funcionamento, tais etapas determinam a arquitetura de reconhecimento facial a ser empregada.

Para a realização de uma técnica de reconhecimento facial que faz uso do algoritmo Viola-Jones, PCA (Análise de Componentes) e *Eigenface*, características estas que serão descritas em subseções seguintes, é necessário realizar os passos a seguir, os quais estão exemplificados na Figura 14.

- **Aquisição das imagens:** Obter as imagens as quais serão processadas. Esta obtenção poderá ocorrer de forma estática, fazendo uso de uma foto, ou de forma dinâmica, fazendo uso de um vídeo obtido por um webcam, lembrando que a obtenção por vídeo difere-se da obtenção estática somente pelo fato de estar processando mais de um quadro, pois um vídeo ou imagem dinâmica é composto por uma sequência de quadros.

- **Pré-processamento:** No intuito de normalizar a imagem. Nesta etapa, a imagem será convertida para a escala cinza (*grayscale*) e normalizada, tal conversão é necessária, pois os processos futuros não necessariamente farão uso das cores para uma comparação.
- **Extração de características:** Obter as características que serão a base para a classificação e verificação.
- **Classificação e Verificação:** Classificar a face como conhecida (autentica) ou desconhecida (impostora).

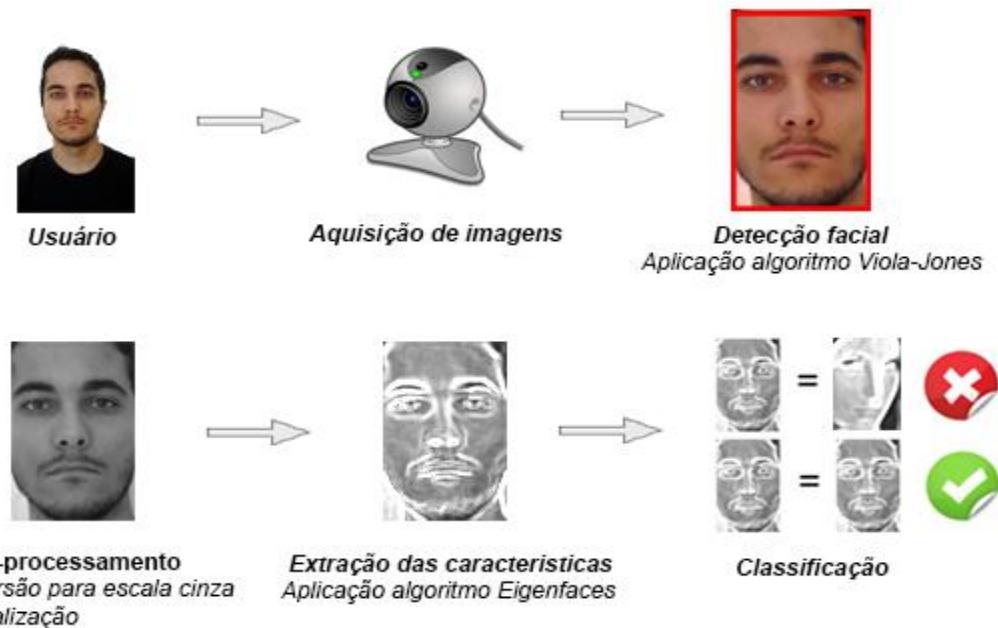


Figura 14 - Exemplo da arquitetura de um sistema de reconhecimento facial.
Fonte - Diniz et. al. (2013). Adaptado.

O processo de reconhecimento facial se dá a partir da aquisição da imagem a qual é obtida através de um webcam, onde o sistema captura a imagem da face do usuário que será a entrada para o sistema de reconhecimento facial, nesta etapa pode ser utilizado o algoritmo de detecção facial Viola-Jones, que será descrito na subseção 5.2, este algoritmo busca características que codificam informações faciais em uma imagem.

O próximo módulo diante o reconhecimento facial é o pré-processamento, onde as imagens de face obtidas pelo algoritmo Viola-Jones são corrigidas e normalizadas na intenção de melhorar o reconhecimento facial. Neste processo as imagens têm correções em suas dimensões, resolução, iluminação e cor, transformando-as na escala de tons de cinza (*grayscale*).

Após o pré-processamento, a face normalizada é a fonte para o processo de extração de características buscando encontrar as principais características a serem utilizadas para classificação. Cada imagem de face (*frame*) é transformada em uma matriz $w \times h$, onde w e h representam respectivamente o número de pixels de largura e altura da imagem. Cada pixel da imagem é um componente desta matriz vetorial.

Diniz et al. (2013) citam que devido à alta dimensionalidade dos vetores é utilizado o PCA (Principal Component Analysis) na etapa de classificação, o qual realiza uma análise dos componentes principais de uma imagem. A aplicação do PCA reduz as características da imagem, reduz o custo computacional e melhora a precisão do classificador.

Juntamente com a técnica PCA pode ser feito o uso da técnica *Eigenface*. O algoritmo *Eigenface* fornece um conjunto de vetores de distribuições probabilísticas para solucionar problemas diante a detecção de padrões em imagens; suas características serão mais bem detalhadas na subseção 5.3.1.

Com os recursos de um classificador de padrões, as características extraídas da imagem facial são comparadas com amostras ou modelos do conjunto de treinamento facial, ou seja, serão comparadas a imagens previamente salvas no banco de dados e posteriormente, após esta comparação, as imagens de entrada são classificadas como conhecidas (autênticas) ou desconhecidas (impostoras).

5.2. Detecção facial

Após a aquisição da imagem de entrada é necessário localizar na mesma uma face. Esse processo é denominado segmentação ou detecção facial. Zenicola Braga (2013) afirma que essa etapa é muito importante, pois nessa fase serão eliminadas informações desnecessárias. Se o algoritmo detectar uma face em uma imagem, ela será extraída, para que possa ser analisada separadamente da imagem original, ou seja, a face detectada será a região de interesse (ROI) a ser trabalhada. Dois requisitos são extremamente importantes para se determinar a qualidade de um algoritmo de detecção: a taxa de falsos positivos e a taxa de falsos negativos.

O processo de detecção, por ser a base para obtenção da imagem facial, tem extrema importância na eficácia de um sistema de biométrico, pois qualquer falha nesse processo poderá comprometer por completo o reconhecimento de faces.

Na literatura atual, o algoritmo mais eficaz é o Viola-Jones. Segundo Viola e Jones (2001), tal algoritmo objetiva localizar em uma imagem características que codifiquem

informações do padrão a ser detectado. Esses padrões são baseados nas características de *Haar*, ilustradas na Figura 15, que codificam informações sobre a presença de contrastes orientados entre regiões da imagem.

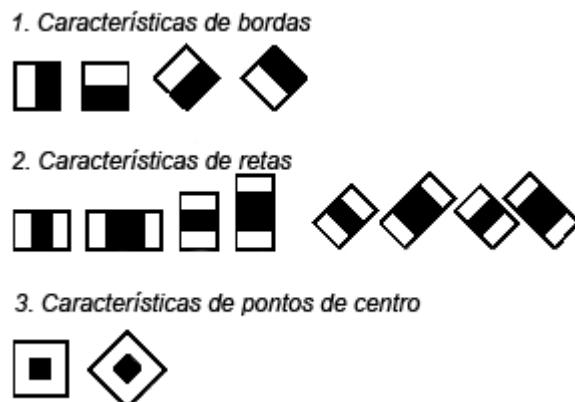


Figura 15 - Características de Haar utilizadas na detecção facial.
Fonte - Viola, Jones (2001). Adaptada.

Ao utilizar os classificadores *Haar* ocorre uma busca por padrões específicos diante os contrastes naturais presentes na imagem, assim como representado na Figura 16.

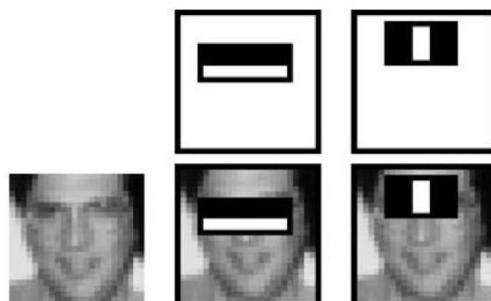


Figura 16 - Padrões faciais encontrados com base em contrastes.
Fonte - Viola, Jones (2001)

Na intenção de computar as características de *Haar* eficientemente, Farina (2012) cita que é gerado uma representação auxiliar da imagem original. Esta representação é chamada de imagem integral, de forma que um pixel (x, y) pertencente a esta imagem, equivale a soma de todos os *pixels* acima e a esquerda do pixel (x, y) do mesmo. Para gerar a imagem integral a partir de uma imagem original utiliza-se a seguinte equação.

$$\begin{aligned}s(x, y) &= s(x, y - 1) + i(x, y) \\ii(x, y) &= ii(x - 1, y) + s(x, y)\end{aligned}$$

Onde ii representa a imagem integral a qual é calculada pela soma de todos pixels a esquerda e acima de $ii(x, y)$, inclusive, e $s(x, y)$ é a soma cumulativa da linha, $s(x, -1) = 0$ e $ii(-1, y) = 0$. A Figura 17 representa a composição do ponto, pertencente imagem integral, que fora obtido pela equação anterior.

Na Figura 17 o quadro (a) representa o valor do pixel $ii(x, y)$ da imagem integral obtido pela soma dos pixels acima e a esquerda dele próprio e o quadro (b) representa a obtenção da região A utilizando o valor dos pontos $L_4 + L_1 - (L_2 + L_3)$.

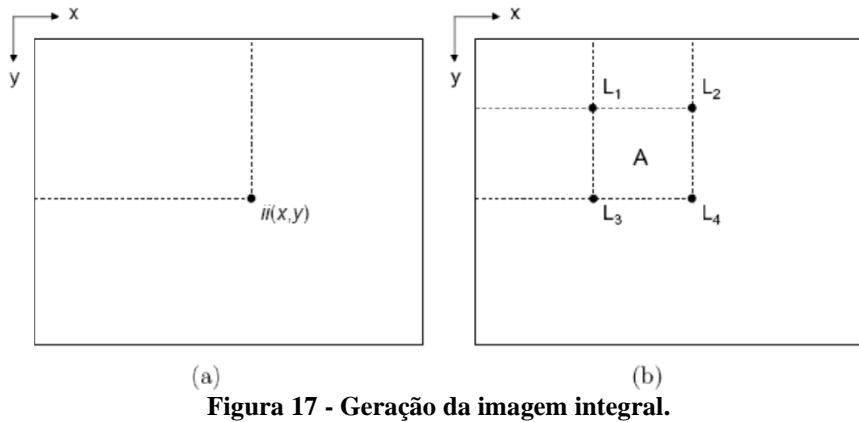


Figura 17 - Geração da imagem integral.

Viola, Jones (2001)

Após a obtenção da imagem integral, conforme citado por Penteado (2009), as características de *Haar* poderão ser computadas em qualquer local ou escala e em tempo constante. Através dos valores dos pixels de ii é possível obter o tamanho de qualquer região da imagem, pois qualquer pixel de ii possui o somatório de linhas e colunas até chegar a si próprio, com isto, para a detecção de um padrão, não é necessário o redimensionamento da imagem e sim somente do detector.

Diante a localização de padrões em uma imagem de qualquer dimensão, o número de combinações das características *Haar* é muito superior ao número de pixels dentro das dimensões de uma imagem, logo, para acelerar o processo de classificação, devem-se manter somente características de maior importância. Para esta necessidade é utilizado o procedimento modificado a partir do método *AdaBoost*, o qual consiste no processo de seleção de características construindo um classificador “forte” com base na combinação de subclassificadores que dependem de uma única característica, os quais são nomeados de classificadores “fracos”.

Na figura 18, um exemplo de detecção facial através de características *Haar*. Neste exemplo, o site *Inspirit* (2014), faz uso da biblioteca *JsFeat* (*JavaScript Computer Vision Library*) para a detecção de padrões faciais existentes em imagens de vídeo.

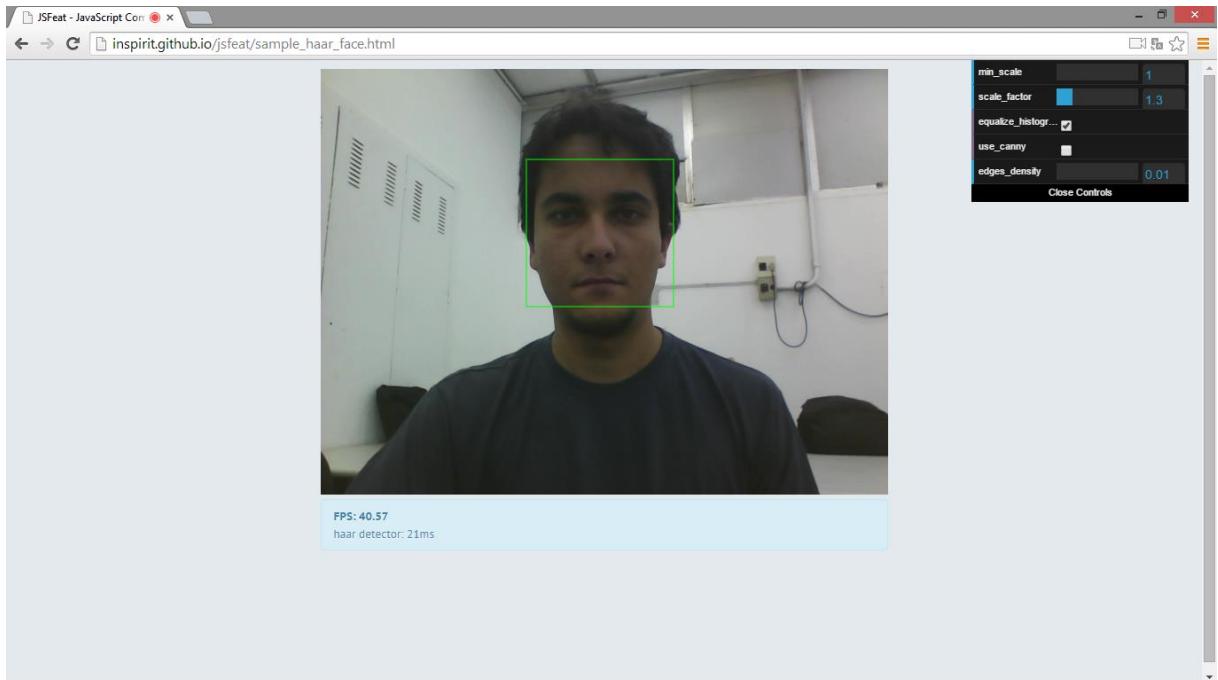


Figura 18 - Detecção facial em vídeo.

Uma importante característica desta técnica está voltada a velocidade de detecção facial, que segundo Penteado (2009), tem resultados positivos independendo de variações nas escalas nas imagens. O conjunto de passos do algoritmo propicia uma detecção muito boa com um tempo de processamento baixo. Por este motivo, esta técnica foi selecionada para esta pesquisa, pois o sistema de reconhecimento facial em caixas eletrônicos deverá ter rápidas respostas evitando atrasos nas transações bancárias.

5.3. Extração de características

Para a classificação de uma face, Diniz et al. (2013) citam a necessidade de extração de características de uma face para reconhecimento da mesma. Tal método pode ser realizado por uma de muitas técnicas, tais como análise de componentes principais (PCA), através do algoritmo *Eigenfaces* ou padrões binários locais (LBP), lembrando que na atualidade, segundo Pereira (2014), já existem outros algoritmos para extração de características tais como o *Deep Learning* (Aprendizado Profundo) utilizado pelo *Facebook*.

Zhao et al. (2003) citam que o processo de comparação facial, o qual é determinado com base nas formas de extração de características da face, é dividido em três tipos.

- **Métodos holísticos:** Usam toda a região da face. Das diversas técnicas existentes a mais utilizada nos métodos holísticos é o PCA. Segundo Zhao et. al. (2003) esta técnica é a mais indicada para com um grande volume de informações presentes em um banco de dados.
- **Métodos estruturais:** Utiliza técnicas mais recentes que fazem uso de medidas geométricas (distâncias e ângulos) relativas a diversos pontos notórios da face, tais como boca, bochechas e nariz.
- **Métodos híbridos:** Buscam oferecer o melhor dos dois métodos anteriormente citados com o objetivo de se aproximar do sistema de percepção humano o qual faz uso tanto da aparência global da face quanto das características locais.

Na seção 5.3.1 será feita uma abordagem da técnica PCA para a extração de características, proporcionando um melhor entendimento dos aspectos da solução proposta.

5.3.1. PCA através da abordagem *Eigenfaces*

Posteriormente a detecção facial é realizada a extração das características da imagem dando andamento ao reconhecimento de uma face, para isto é utilizado nesta pesquisa à transformada de *Karhunen-Loève* ou análise de componentes principais (*Principal Component Analysis*), que segundo Kirby e Sirovich (1990), tem a função de representar imagens faciais de forma comprimida, ou seja, a técnica de análise de componentes principais, também chamada de PCA, desvincula algumas características presentes na imagem, reduz a dimensionalidade dos dados iniciais, conserva as dimensões de maior variância e mantém uma considerável semelhança entre a imagem processada e a imagem não processada.

Devido à alta correlação dos *pixels* de imagens faciais, os dados da face correspondem somente a um subespaço de menor dimensionalidade. O PCA identifica e representa, segundo Li e Jain (2005), este subespaço dimensional através de um vetor de características (vetor de pesos) de baixa dimensionalidade. As informações deste subespaço fornecem informações mais ricas para o reconhecimento facial diferentemente das informações provenientes de uma imagem facial não processada.

A aplicação do PCA pode ser realizada através de uma abordagem diferenciada denominada *Eigenfaces* a qual fora proposta por Turk e Pentland (1991), lembrando que a

criação dos primeiros conceitos desta técnica fora proposta por Kirby e Sirovich (1990) através da análise de componentes principais (PCA).

Turk e Pentland (1991) realizaram o uso da técnica *Eigenfaces* para a classificação de faces e segundo os mesmos a transformada de *Karhunen-Loève* ou PCA é utilizada para obter os vetores que melhor descrevem a distribuição de imagens dentro de um espaço. Estes vetores descritivos são denominados *Eigenfaces* devido à semelhança que possuem com as imagens da face. Na Figura 19 é possível visualizar a notória semelhança entre a face original e a face obtida após a aplicação do PCA.



Figura 19 - Semelhança entre imagens originais e imagens processadas após aplicação de PCA.

Diniz et al.(2013), cita que a técnica *Eigenfaces* é muito semelhante ao PCA, diferenciando-se no fato de que o *Eigenfaces* possui otimizações para a redução da matriz de covariância. Tal diferença proporciona uma redução do processamento necessário para a obtenção de seus autovetores e autovalores da matriz de covariância.

Segundo Kinuta et al. (2013), a obtenção dos vetores que descrevem a distribuição de imagens dentro de um espaço é realizada da seguinte forma.

Dado uma coleção de m imagens de treinamento identificáveis, cujo tamanho matricial é conhecido por $n \times o$; cria-se uma matriz X_{ij} , onde $j = \{1,2,3,\dots,m\}$ representa a quantia de imagens de treinamento e i é o tamanho das imagens em formato vetorial, ou seja, $i = n \times o$, realizar.

- Obtenção da face média (fm).

$$fm = \sum_{r=1}^j X_{ir}, i = 1,2,3, \dots, (n \times o)$$

- b) Centralizar os vetores da imagem realizando uma subtração para cada vetor X encontrado, onde o minuendo equivale ao vetor encontrado e o subtraendo equivale à face média.

$$\bar{X} = X - fm$$

- c) Computar a matriz de covariância.

$$\Lambda = M * M^T$$

- d) Calcular os k autovetores, v_k da matriz de covariância correspondente aos k maiores autovalores λ_k . Os autovetores, em outras palavras, representam imagens que estão agrupadas em uma matriz W com k colunas.

$$\begin{aligned} W_{ik} &= \{v_1, v_2, v_3, \dots, v_k\} \\ \lambda_k &= \{\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n\} \end{aligned}$$

- e) Projetar cada imagem de treinamento em um espaço k -dimensional, gerando um vetor de tamanho reduzido para cada imagem e desta forma, como já mencionado, facilitar a comparação entre os vetores. A projeção é obtida pela multiplicação de cada um dos vetores de imagem pelo autoespaço.

$$\hat{X} = W \cdot \bar{X}$$

Os autovalores mais elevados da matriz de covariância tendem a não serem fixos. Após os cálculos de *eigenfaces* realizados no banco de imagens faciais, realiza-se a classificação (reconhecimento).

Para a classificação adota-se uma imagem R , projetada em um autoespaço, centralizada, com os mesmos valores de média de face obtidos das imagens de treinamento. Esta imagem é classificada com as imagens de treinamento projetadas, através de um classificador específico ou fazendo uso de métodos híbridos para avaliar se a imagem de entrada corresponde a determinado modelo, o que irá classificá-la para uma entidade definida tornando-a autêntica, caso contrário, se a imagem não possuir correspondência será uma imagem impostora sem classificação.

5.4. *Frameworks* para reconhecimento facial

Para possibilitar uma junção de vários métodos de processamento de imagem e visão computacional surgiram frameworks para dar suporte ao desenvolvimento em várias linguagens de programação. Tais *frameworks* tem a função de universalizar técnicas aumentando a produtividade no desenvolvimento de sistemas que fazem uso do processamento de imagem. Como consequência do seu uso, surgem comunidades de desenvolvimento que se auxiliam diante dúvidas para com implementações e conceitos de visão computacional, proporcionando o progresso destes *frameworks* e o surgimento de novas técnicas para processamento de imagem.

5.5. OpenCV

Biblioteca de código aberto que visa auxiliar técnicas de processamento de imagens. Conforme citado no site OpenCV (2014), sua existência é motivada pela criação de uma infraestrutura comum entre aplicações de visão computacional. OpenCV é composto por mais de 2500 algoritmos que permitem a detecção de objetos em imagens, detecção e reconhecimento facial, detecção de movimento dentre outros. Dados provenientes do site OpenCV documentation (2014) citam que sua comunidade é composta por 47 mil pessoas e tem uma estimativa de 7 milhões de downloads.

OpenCV é adotado por diversas empresas tais como Microsoft, Google, IBM e outras sendo que suas funcionalidades estavam presentes em populares sistemas tais como o *Google StreetView*.

Possuem interfaces em C++, C, Python, Java e Matlab, fazendo uso de diversas funções específicas para o processamento de imagens as quais podem ser exemplificadas por.

- **cvLoadImage:** carregar imagem do disco.
- **cvCreateImage:** criar uma imagem.
- **cvShowImage:** Exibe uma imagem na tela.
- **cvSaveImage:** Salva uma imagem em disco.
- **cvQueryFrame:** Responsável por adquirir frames em sequência.

5.6. EmguCV

Conforme o site Emgu (2014), EmguCV ou simplesmente Emgu é um uma plataforma cruzada inteiramente desenvolvida em C# permitindo fazer uso das bibliotecas do OpenCV juntamente com outras linguagens tais como C#, VB etc, em outras palavras o EmguCV é um *Wrapper* que chama funções próprias do OpenCV. Pode ser executada em muitas plataformas tais como Windows, Linux, MacOS, IOS e Android. Em sua estrutura de arquivos possui exemplos de códigos em mais de uma linguagem os quais podem ser exemplificados por algoritmos de reconhecimento de placas veiculares, detecção de textos em imagens e um exemplo de segmentação de faces em imagens.

O EmguCV foi escolhido como ferramenta auxiliar diante esta pesquisa por fornecer características que auxiliam a implementação de técnicas de visão computacional e reconhecimento facial na linguagem C# através do *framework .NET*.

Para o uso desta plataforma existem diversos métodos próprios e outras funções que permitem acesso as bibliotecas do OpenCV. Dentre os principais métodos e classes seguem alguns exemplos.

- **CvInvoke** – Classe cujos métodos realizam chamadas a funções do OpenCV.
- **_EqualizeHist** – Método que realiza uma equalização no histograma da imagem.
- **CascadeClassifier** – Classe que permite, através de seus métodos, detectar um classificador em cascata em uma imagem.
- **Convert** – Método que converte uma imagem para outros tipos, como exemplo a conversão de uma imagem RGB em *grayscale*.

6. PLANEJAMENTO DO PROTÓTIPO

O objetivo deste trabalho é propor a técnica de reconhecimento facial como forma de autenticar usuários de caixas eletrônicos por meio de suas características faciais. Para demonstração da aplicação da técnica de reconhecimento facial na segurança dos caixas eletrônicos, e proporcionar mais segurança aos usuários, será desenvolvido um protótipo denominado *KeyFace* (Face chave). Este protótipo simula o acesso de clientes aos serviços bancários detectando-os pela face.

Primeiramente no subitem 6.1 é feita uma abordagem do planejamento do desenvolvimento do protótipo; no subitem 6.2 são abordados estudos de caso, visando prever situações em que o protótipo será submetido.

O protótipo é dividido em dois módulos de funcionalidades distintas. No primeiro módulo, denominado administrativo, é por onde, por meio de um funcionário da instituição bancária, o cliente é cadastrado. No outro módulo do protótipo, denominado operacional, é simulado o acesso de um cliente a um caixa eletrônico, sendo seu acesso permitido através da verificação do número da conta, senha e face.

Não são abordadas neste protótipo, algumas exceções, como exemplo, quantas vezes o cliente poderá tentar acessar o sistema após ter seu acesso negado. O objetivo central é demonstrar a capacidade do protótipo de detectar uma face e compará-la com amostras armazenadas pelo treinamento, e como resultado dessa comparação, verificar se o indivíduo que está tentando acessar o caixa eletrônico, é o titular da conta.

6.1. Módulo Administrativo

Neste módulo ocorre o cadastramento dos clientes. Aos clientes cadastrados é atribuído um número de conta e uma senha. Neste módulo também é detectado um conjunto de imagens faciais do cliente e armazenado como amostra, para que toda vez que um determinado cliente tente acessar sua conta corrente, o sistema irá detectar a face de quem estiver tentando acessar os serviços, extraíndo suas características faciais, e comparando-as com as amostras previamente armazenadas.

Todas as atividades de cadastros e treinamento, são de responsabilidade de um funcionário do banco.

Para representar todo processo de cadastramento e armazenamento das amostras de imagem dos clientes, foi utilizado o diagrama de atividade, cada etapa do cadastramento é denominada de atividade e é representada na Figura 20.

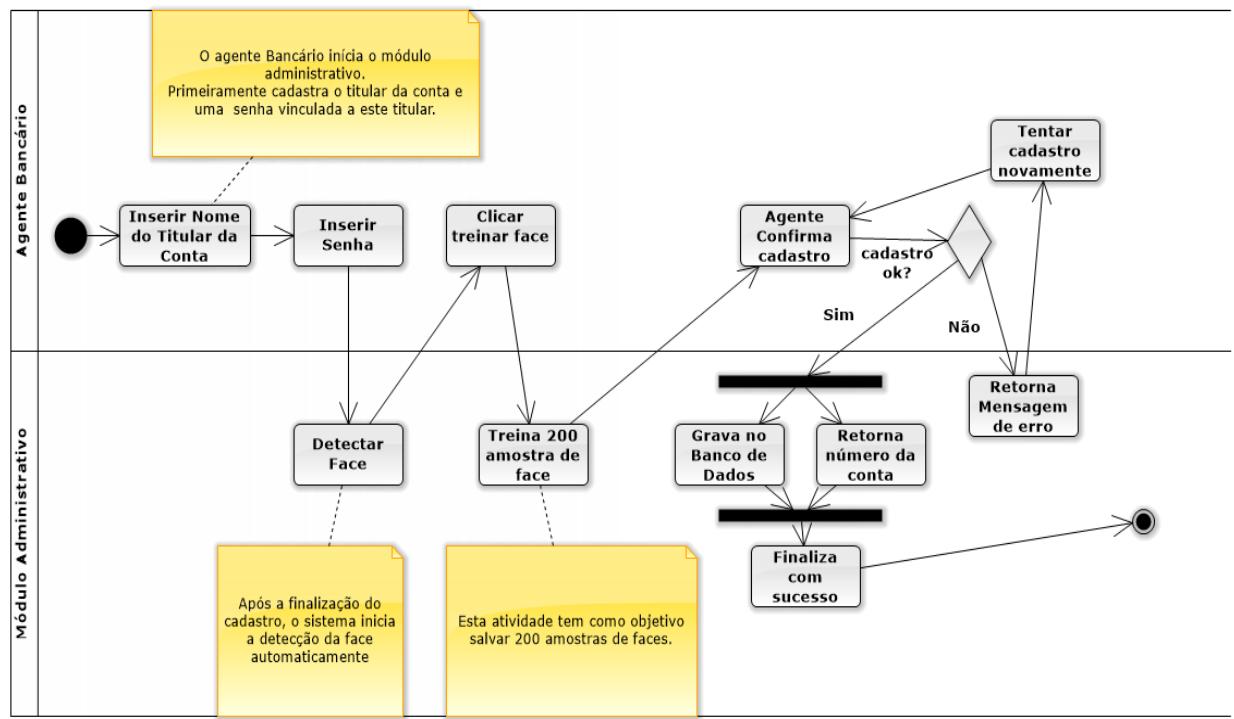


Figura 20 - Representação do processo de cadastrar senha e treinamento de faces.

Ao iniciar o módulo administrativo, o agente bancário irá dispor de um formulário de cadastro; neste formulário é necessário cadastrar o nome e a senha do futuro correntista. Após a efetivação do cliente que está sendo cadastrado, o agente bancário ao clicar em um botão, para que o sistema inicialize o treinamento de faces. Esta função “treinar faces”, armazena 200 amostras de faces do cliente que está sendo cadastrado. Após todo este processo o funcionário deve clicar no botão cadastrar para inserir o correntista no banco de dados juntamente com seus dados cadastrais (nome, senha bancária e amostras faciais). Após o cadastramento do cliente o sistema retorna o sucesso da operação juntamente com o número da conta do correntista ou a falha no cadastramento do usuário que pode ser proveniente de um não preenchimento de campos ou uma falha na comunicação com o banco de dados.

6.2. Módulo Operacional

Módulo operacional é onde ocorre o acesso do cliente. Ao acessar o sistema, é necessário que o cliente informe o número da conta e a senha correspondente a essa conta. O

sistema verifica a correspondência da senha com a conta, se não for verdadeiro, o usuário é redirecionado ao início da operação novamente. Se for verdadeira a detecção de face se inicializará automaticamente. O protótipo irá verificar se a face que ele está recebendo como entrada corresponde a amostra de face armazenada no banco de dados. Simultaneamente é armazenada a face de entrada, mesmo que esta face não corresponda com a amostra de face já anteriormente treinada e armazenada. O intuito do armazenamento é gerar um histórico de tentativas de acesso a determinada conta. Caso não haja correspondência entre as faces comparadas, o sistema direciona o cliente para o início da aplicação. Caso o resultado da comparação seja positivo, o sistema disponibiliza o menu de operações para que o cliente selecione a opção desejada. No diagrama representado na Figura 21 está presente o processo de tentativa de acesso.

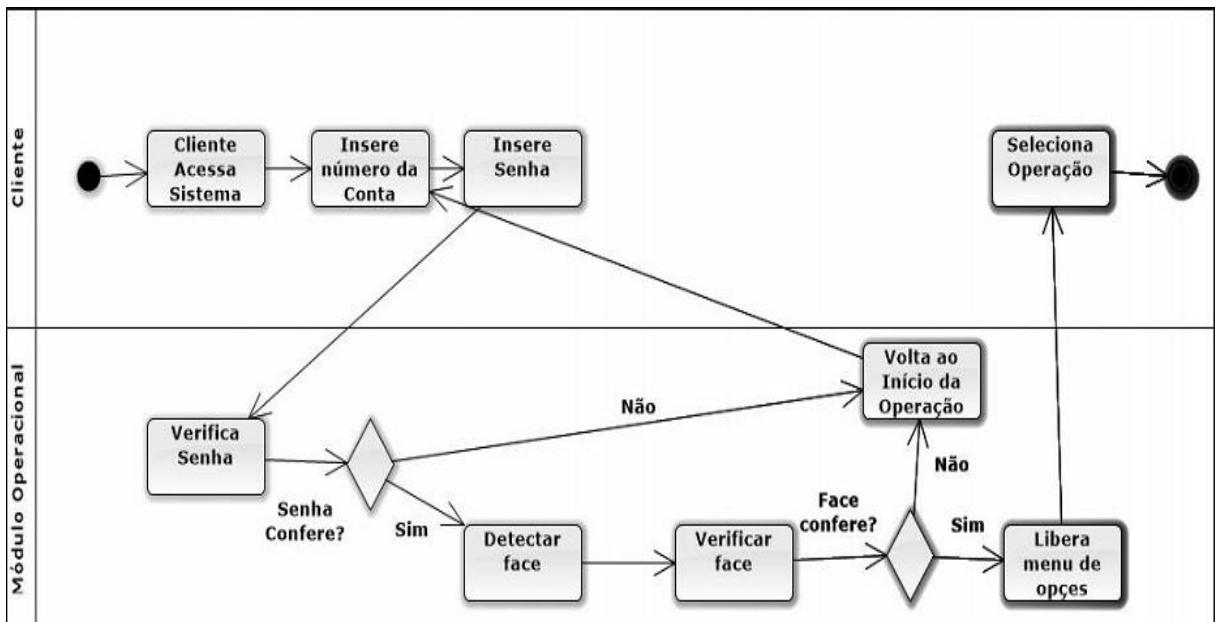


Figura 21 - Fluxo normal processo realizado no modulo operacional

6.3. Estudos de Caso

Estudos de caso referentes às possibilidades as quais o protótipo pode ser submetido durante sua utilização.

6.3.1. Problema do roubo de identidade (clonagem do cartão)

Como descrito no subitem 2.4 do capítulo 2, criminosos encontram várias formas de se subtrair os dados cadastrais de um cliente bancário que é caracterizado como roubo de

identidade. Todas as modalidades de fraudes, como: a troca de cartão, a clonagem da tarja magnética, clonagem de *smart cards* ou quando criminosos se aproveitam de algum descuido dos usuários para aplicar algum tipo de golpe, o que todas tem a mesma finalidade, que é a realização de saques indevidos nas contas de clientes fraudados. No diagrama representado pela Figura 22, está representado como o protótipo se comporta em uma tentativa de autenticação proveniente de um usuário impostor. No cenário descrito no diagrama, o impostor possui a senha e o cartão dos reais correntistas obtidos de alguma das formas de fraudes citadas no capítulo 2, mas através do protótipo *KeyFace*, cujos objetivos são assegurar o correntista, será impossibilitado de efetuar operações no caixa eletrônico, pois sua face não condiz com a face do real correntista.

Os usuários impostores e autênticos terão suas faces armazenadas no banco de dados, ou seja, caso ocorra um falso positivo haverá a possibilidade de verificar as pessoas (faces) envolvidas no processo e assim constatar possíveis criminosos que tentam aplicar o roubo de identidade.

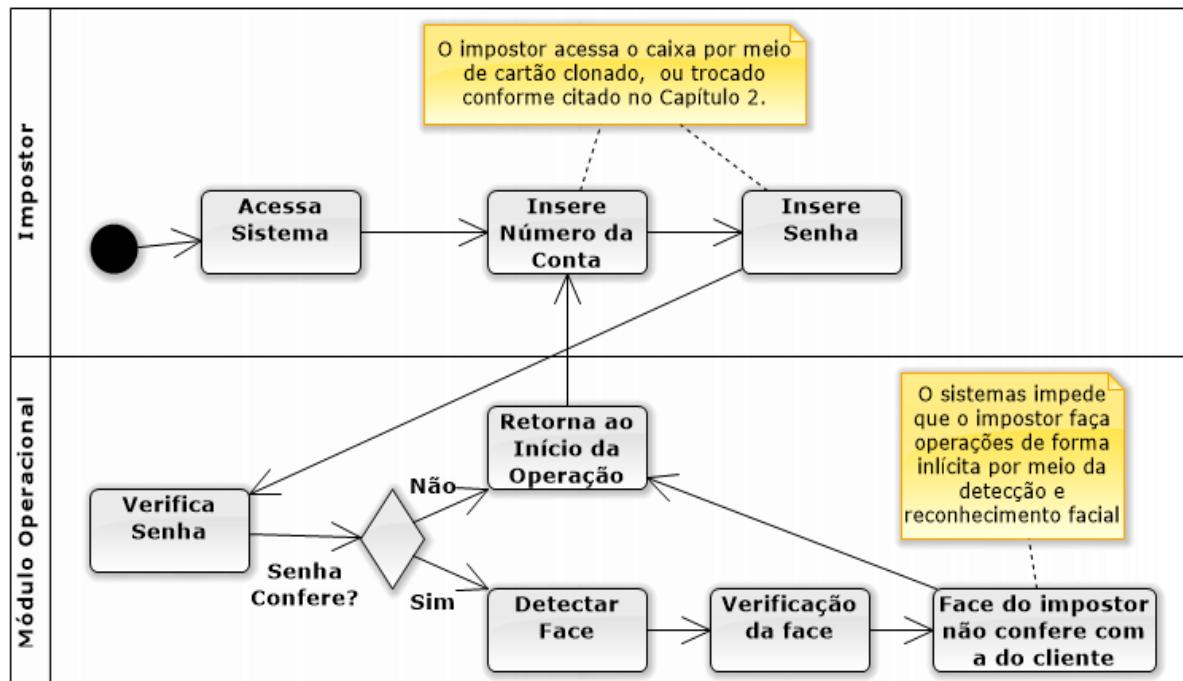


Figura 22 - Representação da tentativa de acesso por um impostor

6.3.2. Esquecimento de senha

Um possível usuário em posse do cartão, caso tenha esquecido sua senha não será submetido a detecção (segmentação) e reconhecimento facial, pois estes últimos processos

são totalmente dependentes de uma validação onde a senha equivale a conta, logo, sem a senha não existe a possibilidade de autenticação e nem mesmo a autenticação por biometria facial. O acesso sem a utilização de senhas não é abordado pelo protótipo, contudo poderá ser uma implementação futura a qual possibilitará ao correntista autenticar-se nos caixas eletrônicos somente com o seu cartão e sua respectiva face. Na Figura 23 é demonstrado o que ocorre quando o usuário acessa sem a senha correta.

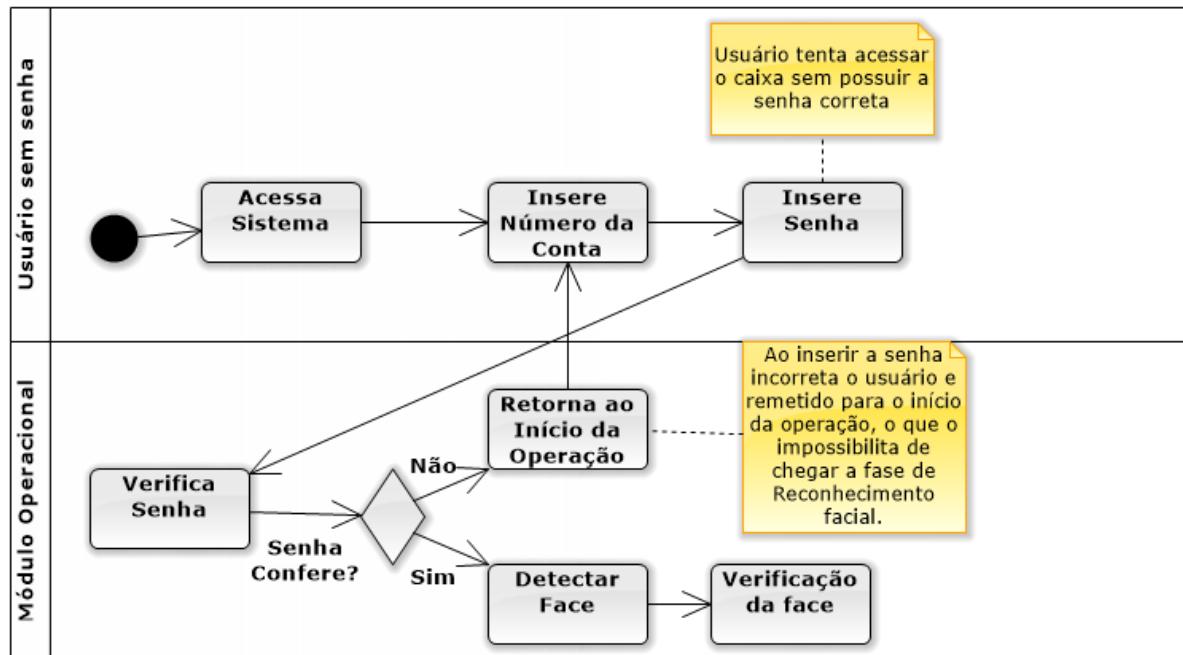


Figura 23 - Demonstração do comportamento do protótipo ao ser acessado com senha incorreta.

6.3.3. Perda do cartão

Em caso de ausência do cartão ou no caso do protótipo *KeyFace*, o esquecimento do número da conta, o usuário é impossibilitado de se autenticar no protótipo, pois o mesmo requere a senha e posteriormente a autenticação facial. Pelo fato deste protótipo operar no modo de comparação um para um (1:1), impede que usuários acessem o protótipo sem o número da conta, o que necessitaria de uma busca no banco de dados comparando um para muitos (1:n). Para trabalhos futuros um cliente sem cartão e sem senha, poderia ter acesso ao sistema somente pela detecção e reconhecimento da face.

6.3.4. Falsos negativos decorrentes de alterações faciais

Um usuário teoricamente autêntico, possuindo cartão e senha, contudo com alterações faciais que o diferem das amostras anteriormente capturadas, ou seja, usuários que possuem hematomas, barba, alterações nos aspectos capilares, usam óculos e alterações na umidade da pele (transpiração), podem não ser autenticados quando tais características não condizem com as características presentes nas imagens obtidas pelo processo de treinamento. No caso de um falso negativo o cliente deve comunicar a instituição bancária para que haja um recadastramento facial, ou seja, uma alteração dos dados faciais do mesmo, podendo aumentar o número de amostras treinadas e consequentemente minimizar as taxas de falsos negativos que podem ser provenientes de um treinamento influenciado por questões luminosas ou até mesmo características faciais defasadas. A possibilidade de alteração das amostras faciais será abordada em futuras implementações do protótipo.

6.3.5. Falsos positivos decorrentes de semelhanças faciais.

Caso um usuário impostor seja semelhante ao usuário real, como exemplo a possibilidade de existirem gêmeos univitelinos, em posse de cartão e senha, faça uso do protótipo o mesmo poderá ser autenticado, contudo deve-se ressaltar como dito no capítulo 1.1, que a senha é pessoal e intransferível.

6.3.6. Auxílio de um terceiro para realizar transações no caixa-eletrônico.

Muitas vezes deficientes, gestantes, idosos e outras pessoas por questões próprias necessitam que outra pessoa realize transações em suas contas e devido a este fato, como implementação futura, será possível cadastrar mais de uma face para uma mesma conta tornando possível o gerenciamento de contas realizado por terceiros. Nos moldes atuais do protótipo ocorre a autenticação, ou seja, uma relação de um para um (1:1) não abordando a verificação que necessitará de uma busca de um para muitos (1:n). Esta implementação futura abre margens para implementação de contas conjuntas às quais necessitam de mais de uma face cadastrada.

6.4. Adequação da infraestrutura para o reconhecimento facial

Visando adaptar os caixas eletrônicos para uso de uma câmera que capte as imagens é necessário nos atentarmos a cadeirantes os quais, por questões físicas, não podem ser visualizados por uma câmera posicionada no topo da estrutura do caixa eletrônico, logo, seria necessária uma adaptação da altura da câmera abrindo novas possibilidades para implementações futuras onde, através da detecção facial, pode ser feito o uso de uma câmera móvel que siga a face do correntista.

Para a correta detecção, o armazenamento de amostras treinadas e reconhecimento facial, são interessantes que haja um melhor controle sobre a iluminação do ambiente, pois a técnica *Eigenfaces*, como dita no capítulo 5, pode ser influenciada por questões luminosas. Outro fator que merece destaque é que a presença de duas faces detectadas impossibilita a autenticação do real correntista, logo, é interessante um ambiente controlado para a realização do reconhecimento facial.

6.5. Delimitações da solução proposta

Algumas fraudes tais como instalação de chupa cabras e outras não serão abordadas pelo resultado proposto, pois envolvem questões externas ao gerenciamento do caixa eletrônico e não serão abordadas por não ser o principal foco da pesquisa, contudo, as consequências de algumas destas fraudes tais como clonagens de cartão que acarreta no roubo de identidade serão focadas e minimizadas.

6.6. Configuração do protótipo

Para que o protótipo tenha resultados satisfatórios, será necessário realizar algumas configurações a fim de ajustá-lo e assim permitir a coleta de dados. Seguem alguns parâmetros que devem ser verificados e ajustados, para que o protótipo tenha uma melhor eficiência.

Threshold - Determina um limiar de aceitação entre a imagem de entrada e a amostra facial cadastrada. Este valor define a distância máxima necessária para classificar a imagem como genuína ou impostora. Valores grandes como 5000 vão fazer a *classifier* retornar a

correspondência mais próxima, mesmo que a probabilidade de que a pessoa tenha sido reconhecida seja muito pequena.

McvTermCriteria - É uma classe que representa a estrutura *EmguCV* para terminar algoritmos iterativos. Ele é composto por dois parâmetros, sendo que o primeiro determina o número de iterações e o segundo, a precisão exigida. Esta classe vai determinar quando as interações de verificação devem parar. A precisão configurada neste objeto deverá ser ajustada para a obtenção de melhores resultados. Inicialmente o número de interação será igual ao número de amostras coletadas.

Tamanho da imagem - Verificar se o tamanho da imagem irá influenciar na capacidade do protótipo, diante o reconhecimento dos clientes, já que é possível configurar o tamanho desejado. Supõe-se que as imagens maiores possuem resoluções melhores, ou seja, teoricamente imagens com dimensões maiores serão melhores quando o quesito é detalhe.

Quantidade de amostras - Amostras são imagens dos clientes coletadas durante o cadastramento da conta e senha. Durante esse cadastramento é feito o treinamento do algoritmo para que posteriormente, ele reconheça determinado cliente que tentará acessar o caixa eletrônico. A cada treinamento é armazenada dez imagens, e o treinamento pode ser feito quantas vezes forem necessários. Antes da coleta de dados será necessário verificar quantos treinamentos serão necessários para obter uma verificação eficiente. Inicialmente serão realizados testes com dez imagens.

Distância da webcam - Verifica qual distância a webcam deve estar em relação ao usuário que está sendo cadastrado ou verificado, e se a distância influencia na qualidade do treinamento e da verificação.

6.7. Coleta de dados

A coleta de dados foi realizada por meio de inserção de dados reais. Foram captadas imagens de pessoas voluntárias para os testes, com prévia autorização por escrito. A coleta de dados tem como objetivo, avaliar o funcionamento do protótipo, bem como verificar se atende os objetivos declarados no capítulo 1. O objetivo da coleta de dados, também é analisar o tempo que o protótipo leva para fazer a verificação do indivíduo que está tentando acessar o caixa eletrônico, e se é viável aplicá-lo a um caixa eletrônico.

Foi feito levantamento do percentual de falsos negativos e falsos positivos, que é quando um cliente é autenticado como impostor erroneamente e quando um impostor é autenticado como cliente, respectivamente.

Como citado no Capítulo 5, a luminosidade do ambiente pode influenciar os resultados. Com isso o protótipo foi testado em ambientes de tons de luminosidade diferentes.

Foram verificadas quantas iterações é necessário para que a verificação seja eficiente. Como já citado no tópico 6.6, a coleta de dados foi realizada com número de iterações igual ao número de imagens armazenadas.

Também foi feito levantamento do percentual no qual o protótipo identifica ou recusa o usuário logo após a confirmação de que a conta e a senha são verdadeiras. Verificar qual percentual iremos determinar ao protótipo para que ele aprove o acesso e em qual percentual haverá recusa.

Também verificar se em uma determinada configuração do protótipo, há alguma variação nos resultados obtidos.

Por fim, verificar se quando o indivíduo no momento da verificação estiver em movimento, prejudica sua identificação.

Para facilitar a coleta de dados, o protótipo foi projetado de forma que seja possível visualizar, tanto módulo administrativo como no módulo operacional, alguns dados que vão nos permitir avaliá-lo, como: a quantidade de imagens treinadas, a média de tempo que leva pra uma face ser detectada, quantos quadros (ou *frames*) serão utilizados para fazer a verificação, quantidade de imagens reconhecidas, quantidade de imagens que não foram reconhecidas e também o percentual de aprovação.

Todos os dados coletados foram tabulados no aplicativo Microsoft Excel 2010, para geração de planilhas e gráficos, a fim de facilitar a visualização dos resultados obtidos.

7. DEMONSTRAÇÃO DAS FUNCIONALIDADES DO PROTÓTIPO

Este capítulo tem como objetivo demonstrar as funcionalidades do protótipo após o término de seu desenvolvimento e também expor os resultados amostrais obtidos em teste realizados com o mesmo. Este protótipo foi desenvolvido com o único objetivo de demonstrar a técnica de reconhecimento facial, que é o objeto de estudo desta pesquisa. Por se tratar de um protótipo, algumas funcionalidades não foram adicionadas, como alteração de dados cadastrais do cliente (nome do cliente, número da conta, senha e quantidade de amostras), quando for necessário realizar um novo teste, um novo cadastro deve ser realizado.

7.1. Demonstração das funcionalidades Protótipo

O protótipo, como relatado em seu planejamento no Capítulo 6, foi desenvolvido em dois módulos: administrativo e operacional. Será descrito a seguir a execução de cada passo tanto do módulo administrativo como no módulo operacional. Foram utilizadas imagens das telas para melhor ilustrar a execução de cada passo, assim facilitar seu entendimento. Para melhor demostrar o protótipo, algumas informações de comportamento são exibidas diretamente nas telas, isso também irá facilitar seu entendimento.

Para o desenvolvimento dos resultados desta pesquisa foram adotadas ferramentas de apoio que permitissem desenvolver um protótipo para detecção e autenticação facial em curtos prazos. No intuito desenvolver resultados rápidos foi adotado ferramentas *Microsoft* para o desenvolvimento, dentre elas o Microsoft SQL Server para armazenar imagens faciais e informações dos correntistas, pois é uma ferramenta a qual, no momento, tínhamos um maior domínio. Para desenvolvimento do protótipo foi adotada a linguagem C# e a IDE *Microsot Visual Studio*, pois também há maior domínio nas mesmas e com base nisto o desenvolvimento foi mais rápido em relação a outras linguagens e IDEs. Através do framework .Net fizemos uso do modelo ORM utilizando *Entity Framework* para a persistência de dados e desta forma também ganhamos tempo de desenvolvimento, pois não houve a necessidade de criação de *procedures* ou *scripts* SQL apenas fazendo uso de *LINQ to Entities*.

Para a interface gráfica adotou-se o WPF (*Windows Presentation Foundation*), pois é uma tecnologia nova em relação ao *Windows Forms* e ouve interesse de se adquirir conhecimento na mesma. Para apoiar o processamento de imagens fora utilizado o framework *EmguCV* visando que o mesmo integra-se com as *dlls* do *OpenCV* permitindo inúmeras

possibilidades de desenvolvimento para visão computacional em .NET. O *EmguCv* possui fácil integração com o *.NET framework* e apresentou rápidas respostas para as técnicas empregadas. De forma geral as ferramentas foram escolhidas de acordo com o conhecimento técnico dos envolvidos no desenvolvimento do protótipo. O diagrama do banco de dados está representado na Figura 24.

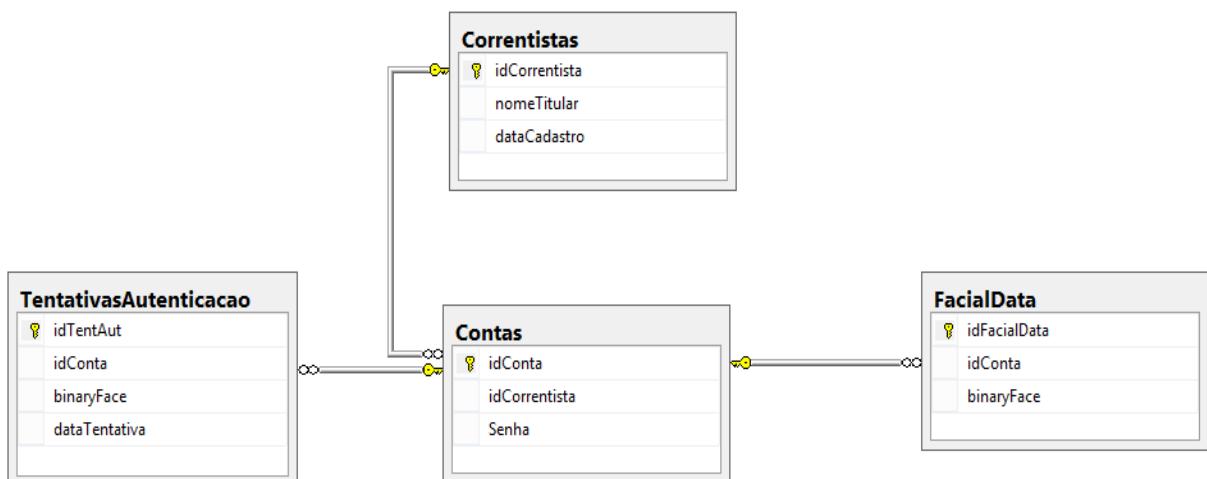


Figura 24 - Diagrama do banco de dados utilizado no protótipo.

7.1.1. Funcionalidades do módulo administrativo

Neste módulo, denominado administrativo, são realizados cadastramentos de clientes e contas. Por meio deste é realizado o treinamento, para que, posteriormente, no módulo operacional seja feita a verificação. Na Figura 25 são demonstrados os itens de funcionalidade e logo após, é feita uma breve descrição de cada item.

- **Item 1 - Aba cadastramento:** Esta aba indica a área do protótipo na qual será realizado o cadastramento.
- **Item 2 - Aba consulta:** Através desta aba é possível acessar a área de consulta, na qual são exibidos os clientes cadastrados.
- **Item 3 - Botão “Iniciar Captura”:** Através deste botão a câmera é acionada e inicia-se a captura de imagens e a detecção de faces.
- **Item 4 - Botão “Parar Captura”:** Através deste botão encerra-se a captura de imagens. Uma observação importante a ser feita, é que no caso deste protótipo, deve-se encerrar a captura

antes da utilização do módulo operacional, já que os dois módulos utilizam a mesma câmera para captura de imagens.

Tela Cadastro

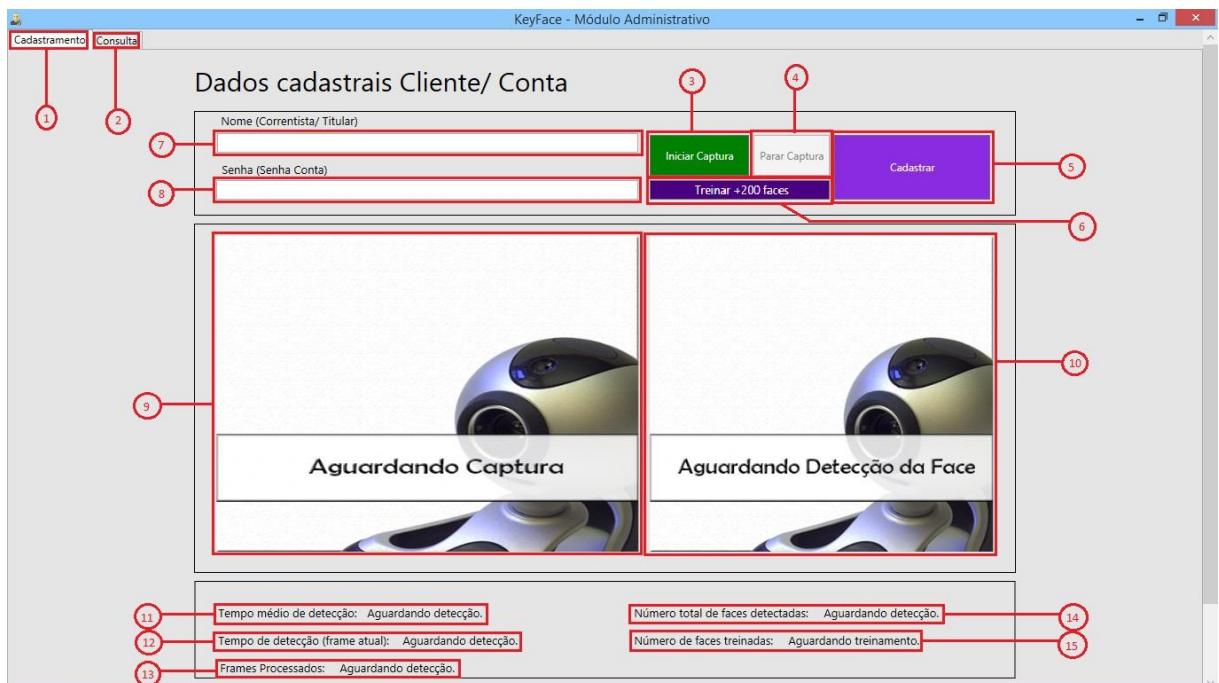


Figura 25 - Tela de cadastro do módulo administrativo.

- Item 5** - Botão “Cadastrar”: Este botão é responsável por inserir registros no banco de dados. Para acionar este botão, é necessário primeiramente, inserir o nome do cliente na caixa de texto indicada no item 7 da Figura 25, inserir a senha do referido cliente na caixa de texto do item 8 da Figura 25 e ter realizado no mínimo um treinamento de imagens no qual é feito por meio do acionamento do botão “treinar + 200 faces”, também indicado na Figura 25, por meio do item 6.
- Item 6** - Botão “treinar +200 faces”: Através deste botão é realizado o treinamento de imagens faciais para que posteriormente o protótipo seja capaz de permitir o acesso de um cliente genuíno ou de impedir o acesso de um impostor. A cada acionamento deste botão, são armazenadas em memória 200 imagens faciais do indivíduo que está sendo detectado através da câmera. Para que seja possível realizar o treinamento, a câmera deve estar ligada, e isto é feito através do botão “Iniciar captura”, que é indicado pelo item 3 da Figura 25.
- Item 7** - Caixa de texto nome: Onde se deve inserir o nome do cliente a ser cadastrado.
- Item 8** - Caixa de texto senha: Onde se deve inserir a senha do cliente a ser cadastrado.

- **Item 9 - Área de detecção:** Nesta área é exibida em tempo real, a imagem que está sendo capturada no momento pela câmera. Caso a câmera esteja desligada será exibida uma imagem estática com a mensagem “Aguardando Captura”, como demonstrado na Figura 26.



Figura 26 - Aguardando Captura.

Com a câmera ligada e sem que esteja ocorrendo a detecção de face, no topo da imagem, será exibida a mensagem “Aguardo sua face”, como demonstrado na Figura 27.



Figura 27 - Aguardando Face.

Após uma face ser detectada, a área determinada como região de interesse, será demarcada por um retângulo vermelho. Somente a área interna ao retângulo será armazenada. Segue exemplo de uma face detectada na Figura 28.

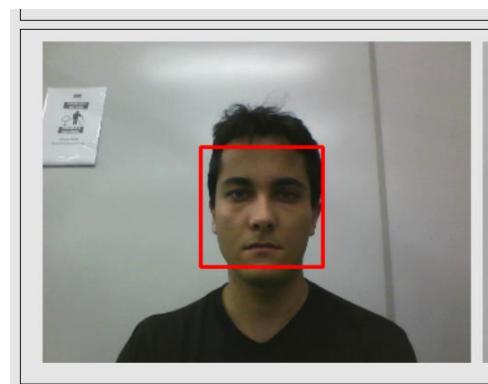


Figura 28 - Face sendo detectada.

Caso mais de uma face seja detectada, todas as faces serão isoladas com o retângulo vermelho, porém não será possível realizar o treinamento de faces, já que o protótipo automaticamente interrompe o treinamento, avisando que existem mais que uma face sendo detectada com a mensagem ao topo do vídeo “2 (ou mais) faces detectadas”. Segue exemplo demonstrado na Figura 29.



Figura 29 – Duas faces Sendo detectadas.

- **Item 10 - Área da região de interesse:** Esta é a área da imagem que realmente será armazenada em banco de dados, para posteriormente se verificar se o cliente que está acessando o caixa eletrônico é realmente genuíno. Caso a câmera esteja desligada ou nenhuma face sendo detectada, será exibida uma imagem estática com a mensagem “Aguardando detecção da face”, como demonstra a Figura 30.



Figura 30 – Aguardando Detecção da Face.

Caso uma face seja detectada, a mesma será exibida na área de região de interesse da face, já convertida para a escala cinza (*grayscale*). Segue exemplo na Figura 31.

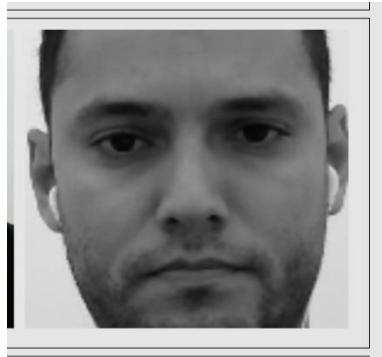


Figura 31 – Área de região de interesse da face.

- **Item 11** - Tempo Médio de detecção: tempo médio em que cada face foi detectada em uma imagem.
- **Item 12** - Tempo de detecção (frame atual): Tempo em que a última face foi detectada em uma imagem.
- **Item 13** - Frames processados: Quantidade de imagens processadas mesmo que nenhuma face fora detectada.
- **Item 14** - Número total de faces detectadas: quantidade de faces detectadas a partir do momento em que a câmera foi ligada.
- **Item 15** - Número de faces treinadas: número de faces armazenadas para posteriormente serem utilizadas na autenticação. Podem ser armazenadas 200 imagens.

Tela Consulta

Esta área do protótipo foi desenvolvida com objetivo de demonstrar as contas pós-cadastro. Nela é possível fazer consultas por nomes dos clientes cadastrados no protótipo. O retorno da consulta será o nome do cliente, o número de sua respectiva conta e a primeira imagem do total de imagens cadastradas para esse cliente. Para selecionar esta área, é necessário clicar no topo da página na aba “Consulta”. Na Figura 32, é mostrado cada componente desta área do protótipo.

- **Item 1** - Caixa de texto nome do cliente: Para uma busca detalhada, basta digitar o nome do cliente desejado. Caso nenhum nome inserido, todos os clientes serão retornados.
- **Item 2** - Botão “Consultar Cliente”: Inicia a consulta.

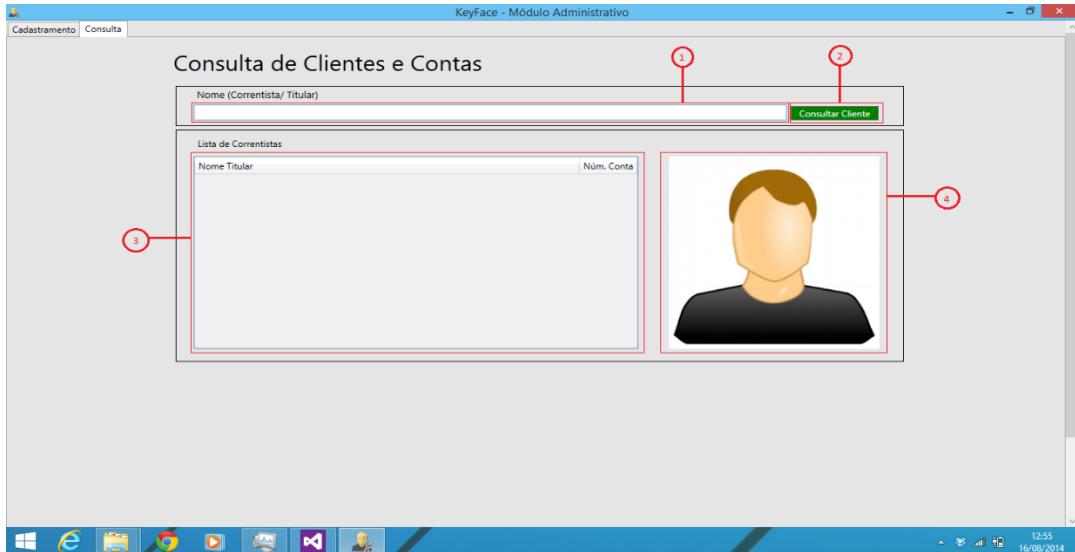


Figura 32 - Tela de Consulta do Módulo Administrativo.

- **Item 3 - Lista de correntistas:** Exibe a lista resultante da consulta. Segue exemplo na Figura 33.

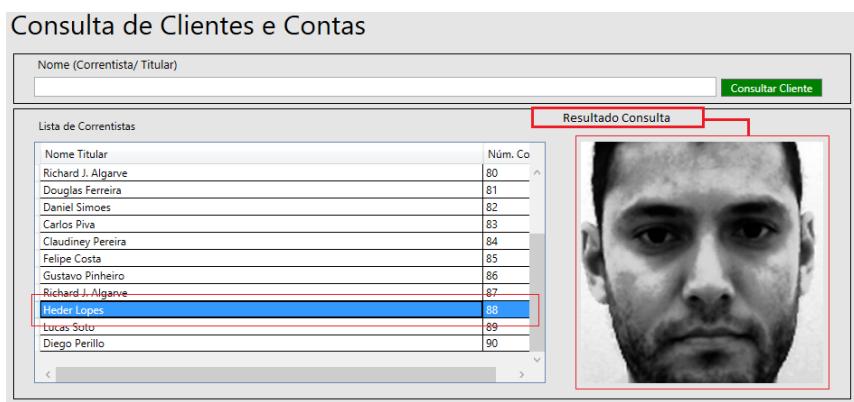


Figura 33 - Resultado da consulta de clientes

- **Item 4 - Imagem:** Imagem do correntista consultado.

7.1.2. Funcionalidades do módulo operacional

Neste módulo será demonstrado o reconhecimento facial como auxiliar do processo de autenticação de clientes nos caixas eletrônicos, ou seja, como complemento do cartão utilizado para acesso e da senha. Segue na Figura 34, a tela inicial do módulo operacional.

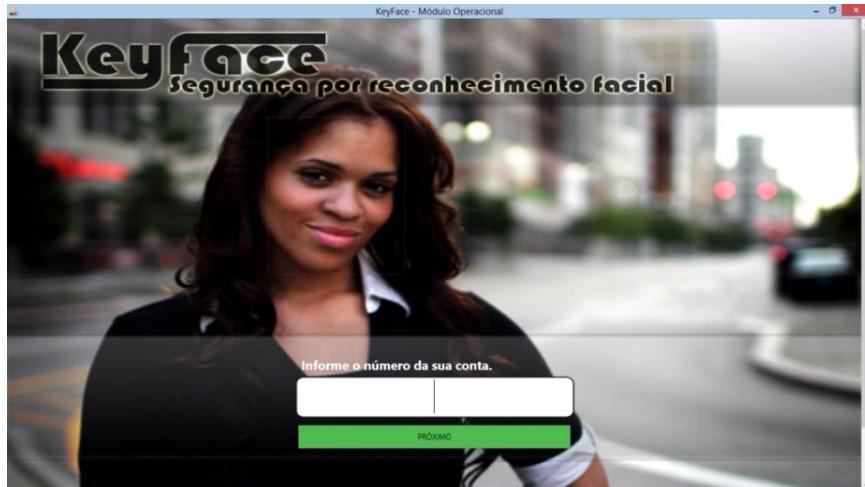


Figura 34 - Tela Inicial do Modulo Operacional

A tela inicial contém uma caixa de texto, solicitando que o cliente informe o número de sua conta. Este número será fornecido logo após o cadastramento do cliente no módulo administrativo, e a inserção deste número, é a simulação da introdução do cartão no caixa eletrônico. Ao inserir o número da conta e clicar no botão “PRÓXIMO”, o protótipo disponibilizará a tela para inserção da senha, como demonstrado na Figura 35.

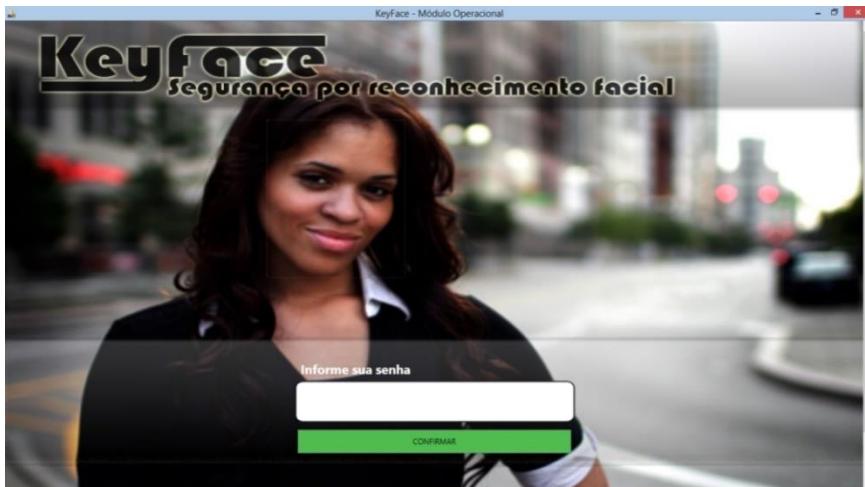


Figura 35 - Tela para inserção da senha.

A tela para inserção da senha tem as mesmas características da tela inicial, porém nela somente será solicitada a senha que foi cadastrada no módulo administrativo e vinculada à conta do cliente. Caso a senha inserida não coincida com o número da conta a qual foi vinculada ou a conta não exista, o protótipo não permitirá avançar para tela de reconhecimento e redirecionará o usuário para a tela inicial. No caso de inserção de conta e senha válida, o protótipo avança para tela de reconhecimento acionando a câmera e automaticamente começa a detectar a face do cliente que está tentando acessar o sistema.

Assim como no módulo administrativo, caso duas faces forem detectadas ao mesmo tempo, o processo é interrompido. Se o cliente não estiver devidamente posicionado para detecção de sua face, no momento do reconhecimento (não esteja na frente da câmera), o protótipo exibirá uma imagem estática com a mensagem “Aguardando detecção da face”. No canto superior direito, é exibido imagem do cliente da referida conta que se está tentando acessar, isso é somente para efeitos de demonstração, como demonstra a Figura 36.



Figura 36 - Imagem do protótipo aguardando face para o reconhecimento.

No caso do cliente estar devidamente posicionado para a câmera que está fazendo a captura de imagens (com a parte frontal da face voltada para a câmera), será feito a detecção da face de entrada, que terá seu contorno marcado em vermelho. Neste momento, um determinado número de faces, denominadas faces de entrada, serão utilizadas pelo protótipo para comparação com as faces armazenadas no momento do cadastramento, no módulo administrativo (no momento “treinar faces”). O número de comparações será n para o número de imagens armazenadas no banco de dados, multiplicados por m , números de faces de entrada ($n \times m$), que resulta no número de comparações realizadas pelo protótipo. Na Figura 37, é demonstrado o momento em que está ocorrendo a comparação.

Para cada imagem de entrada, será gerado o percentual de aprovação resultante das comparações realizadas com as amostras armazenadas no banco de dados. A aprovação do acesso do cliente será fornecida mediante a média do percentual de comparações realizadas com todas as faces de entrada; tal média deve ser maior que um percentual previamente determinado, o qual também representa um limiar entre a ocorrência de falsos positivos e falsos negativos. Se o acesso for permitido, o protótipo disponibilizará a próxima tela, que

representa o menu de operações bancárias. Na Figura 38 é demonstrada a imagem da tela que o protótipo disponibiliza após a permissão do acesso.



Figura 37 - Momento em que a comparação é realizada.



Figura 38 - Menu de operações disponibilizado após permissão de acesso.

8. RESULTADOS OBTIDOS COM A COLETA DE DADOS

Para se chegar aos resultados, foram necessários testes de configuração na coleta de dados. Estes testes foram realizados de forma empírica devido ao número de parâmetros a serem considerados. Foram feitos testes armazenando resoluções de imagens diferentes, alternando a intensidade da iluminação do local dos testes, alternando a distância do indivíduo em relação à câmera e também alternado tanto a quantidade de imagens armazenadas no banco de dados como a quantidade de imagens de entrada utilizadas para comparação.

8.1. Configuração do Protótipo

Os parâmetros de configuração já foram citados no planejamento do protótipo no tópico 6.6 do Capítulo 6. Um dos pontos importantes nos testes, considerados relevantes, foi verificar a distância do cliente em relação à câmera no momento da detecção. Foi verificado nos testes de configuração que, entre uma distância de 1 a 2 metros, a detecção e verificação são eficientes. No que tange a iluminação do ambiente, o mesmo deve estar bem iluminado para resultados mais precisos.

As demais configurações mais apropriadas foram.

- Imagens com dimensões de 200 *pixels* de largura e 200 *pixels* de altura.
- O ambiente deve ser bem iluminado.
- A distância deve ser de aproximadamente 1 metro da pessoa em relação à câmera.
- O *threshold* deve ser elevado para 5000. Visa diminuir ao máximo a rejeição de genuínos.
- O número de iterações do *McvTermCriteria* deve ser fixado em 16 e o parâmetro de precisão (*epsilon*) deve ser fixado para 0,001.
- No cadastramento devem ser armazenadas 200 imagens de amostras e na verificação estão sendo utilizadas 7 imagens.
- O protótipo foi configurado para que, quando reconhecer igual ou superior a 86% das imagens de entrada, o considere genuíno e abaixo desse valor o considere impostor.

Segue na Tabela 3, o resumo das configurações.

Tabela 3 - Parâmetros resultantes do teste de configuração do protótipo.

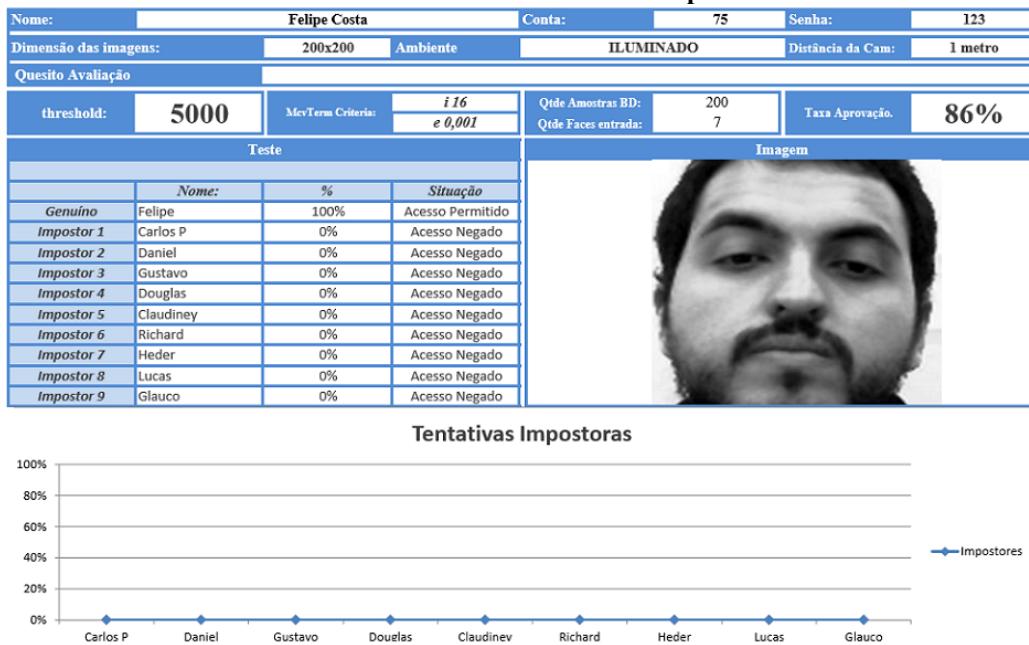
PARAMETRO	VALOR
Dimensão das imagens:	200x200
Ambiente	Iluminado
Distância da câmera:	1 metro
Threshold:	5000
McvTerm Criteria:	i 16 e 0,001
Qtde Amostras BD:	200
Qtde Faces entrada:	7
Taxa Aprovação.	86%

8.2. Resultados do Protótipo

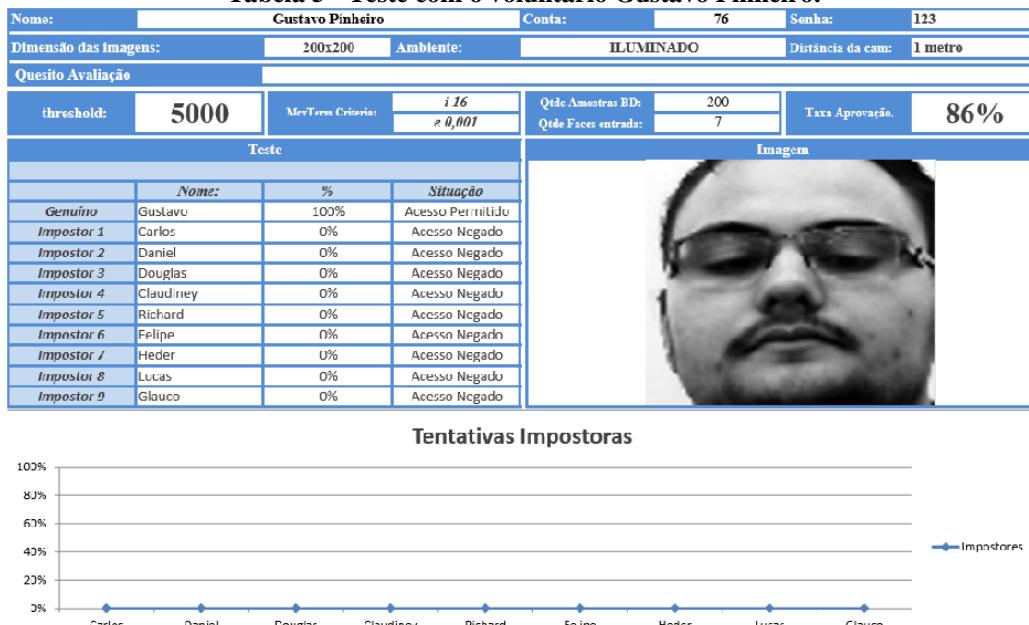
A partir da configuração do protótipo, inicializou-se a coleta de dados. Para um grupo de 10 pessoas, foram realizados os cadastros de 10 contas, uma para cada indivíduo. Assim foram gerados 10 grupos de coletas. Cada grupo de teste contém o registro de tentativa de acesso do proprietário da conta, denominado como genuíno, e também a tentativa de acesso de outras 9 pessoas, denominados como impostores.

Nas tabelas foram registrados os nomes das pessoas que no momento tentava acessar determinada conta (tanto como genuíno ou como impostora), a taxa de aprovação gerada pelo protótipo, resultante das comparações e a situação do cliente resultante do teste. Para serem considerados aptos a acessar o menu de operações, foi determinado que a taxa de aprovação seja maior ou igual a 86%, sendo assim, os genuínos que obtiverem aprovação abaixo dessa taxa, serão considerados falsos negativos, caso contrário sua situação será “Acesso Permitido”. Para os impostores que obtiverem taxa de aprovação igual ou acima de 86%, serão considerados falsos positivos, caso contrário, sua situação será considerada “Acesso Negado”. Da Tabela de 4 à Tabela 13 está demonstrado os 10 grupos de testes realizados.

Na Tabela 4, teste realizado com o voluntário Felipe Costa. O mesmo foi autenticado com 100% de aprovação. Os 9 impostores que tentaram acessar sua conta, tiveram seus acessos negados e nenhuma de suas imagens foram consideradas genuínas. Nenhuma taxa de falso positivo foi gerada.

Tabela 4 - Teste com o voluntário Felipe Costa.

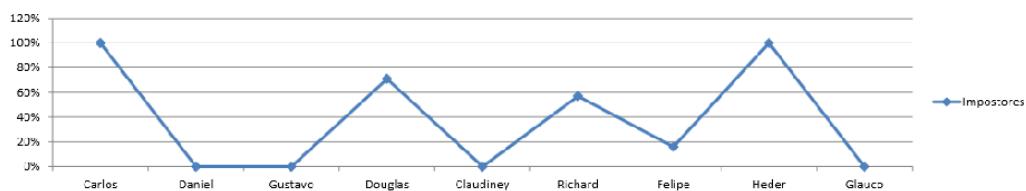
Na Tabela 5, teste realizado com o voluntário Gustavo Pinheiro. O mesmo foi autenticado com 100% de aprovação. Os 9 impostores que tentaram acessar sua conta, tiveram seus acessos negados e nenhuma de suas imagens foram consideradas genuínas. Nenhuma taxa de falso positivo foi gerada.

Tabela 5 - Teste com o voluntário Gustavo Pinheiro.

Na Tabela 6, teste realizado com o voluntário Lucas Soto. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 2 conseguiram acessar sua conta.

Tabela 6 - Teste com o voluntário Lucas Soto.

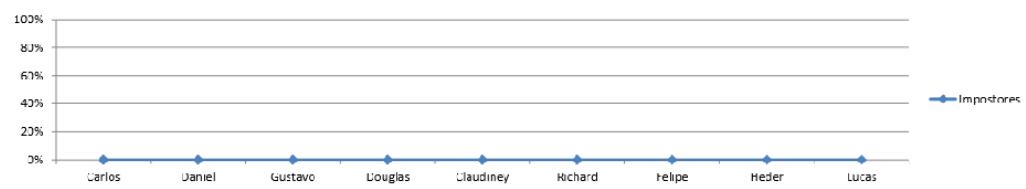
Nome:	Lucas Soto		Conta:	77	Senha:	123
Dimensão das Imagens:	200x200		Ambiente:	ILUMINADO		Distância da Cam:
Quesito Avaliação						
threshold:	5000	MetTerm Critério:	i 16 e 0,001	Qtde Amostras BD:	200	Taxa Aprovação.
Teste						
	Name:	%	Situação	Imagen		
<i>Genuíno</i>	Lucas	100%	Acesso Permitido			
<i>Impostor 1</i>	Carlos	100%	Falso positivo			
<i>Impostor 2</i>	Daniel	0%	Acesso Negado			
<i>Impostor 3</i>	Gustavo	0%	Acesso Negado			
<i>Impostor 4</i>	Douglas	71%	Acesso Negado			
<i>Impostor 5</i>	Claudiney	0%	Acesso Negado			
<i>Impostor 6</i>	Richard	57%	Acesso Negado			
<i>Impostor 7</i>	Felipe	16%	Acesso Negado			
<i>Impostor 8</i>	Heder	100%	Falso positivo			
<i>Impostor 9</i>	Glauco	0%	Acesso Negado			

Tentativas Impostoras

Na Tabela 7, teste realizado com o voluntário Glauco. O mesmo foi autenticado com 100% de aprovação. Nenhum dos impostores conseguiu acessar sua conta.

Tabela 7 - Teste com o voluntário Glauco.

Nome:	Glauco		Conta:	78	Senha:	123
Dimensão das Imagens:	200x200		Ambiente:	ILUMINADO		Distância da Cam:
Quesito Avaliação						
threshold:	5000	MetTerm Critério:	i 16 e 0,001	Qtde Amostras BD:	200	Taxa Aprovação.
Teste						
	Name:	%	Situação	Imagen		
<i>Genuíno</i>	Glauco	100%	Acesso Permitido			
<i>Impostor 1</i>	Carlos	0%	Acesso Negado			
<i>Impostor 2</i>	Daniel	0%	Acesso Negado			
<i>Impostor 3</i>	Gustavo	0%	Acesso Negado			
<i>Impostor 4</i>	Douglas	0%	Acesso Negado			
<i>Impostor 5</i>	Claudiney	0%	Acesso Negado			
<i>Impostor 6</i>	Richard	0%	Acesso Negado			
<i>Impostor 7</i>	Felipe	0%	Acesso Negado			
<i>Impostor 8</i>	Heder	0%	Acesso Negado			
<i>Impostor 9</i>	Lucas	0%	Acesso Negado			

Tentativas Impostoras

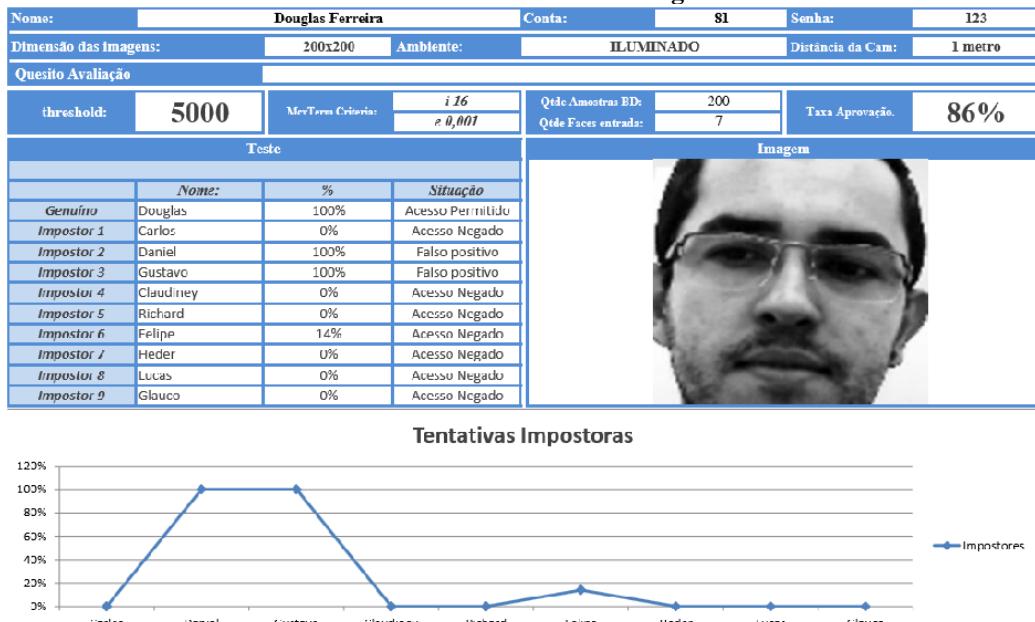
Na Tabela 8, teste realizado com o voluntário Heder Lopes. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 3 conseguiram acessar sua conta.

Tabela 8 - Teste com o voluntário Heder Lopes.

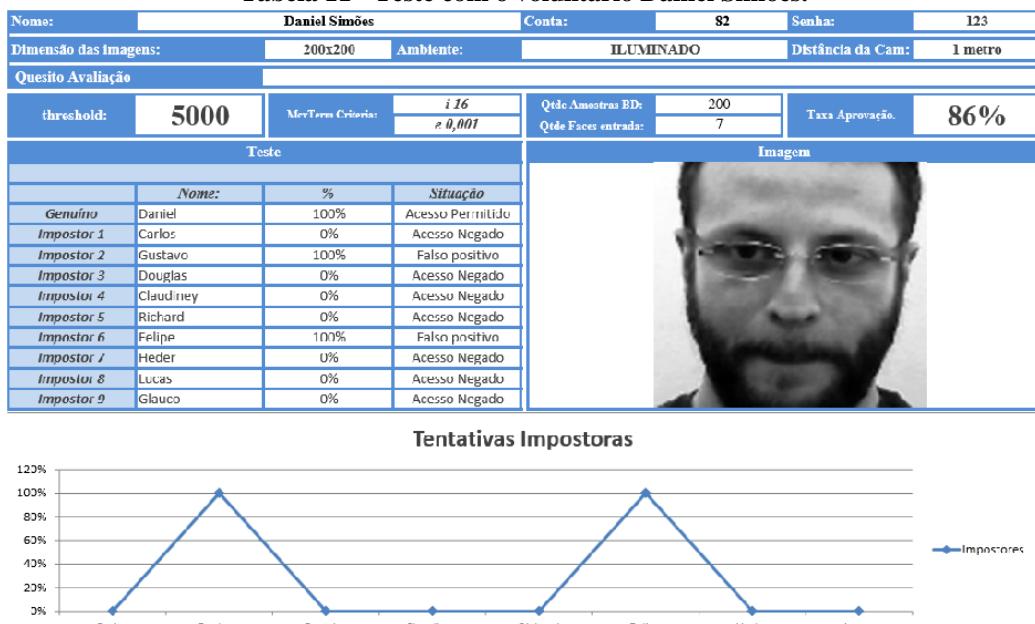
Na Tabela 9, teste realizado com o voluntário Richard Algarve. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 3 conseguiram acessar sua conta.

Tabela 9 - Teste com o voluntário Richard Algarve.

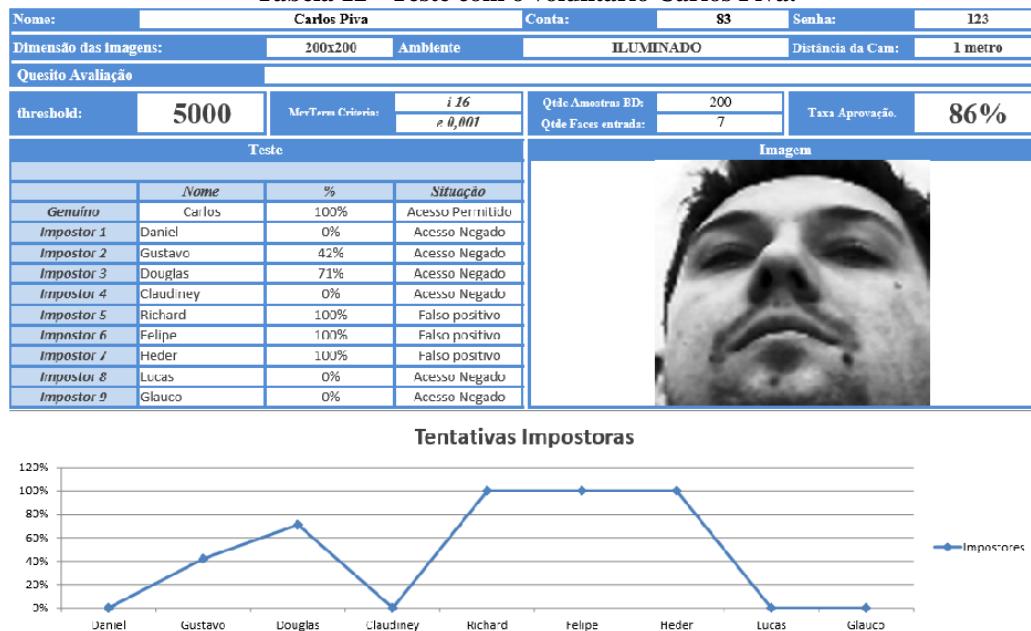
Na Tabela 10, teste realizado com o voluntário Douglas Ferreira. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 2 conseguiram acessar sua conta.

Tabela 10 - Teste com o voluntário Douglas Ferreira.

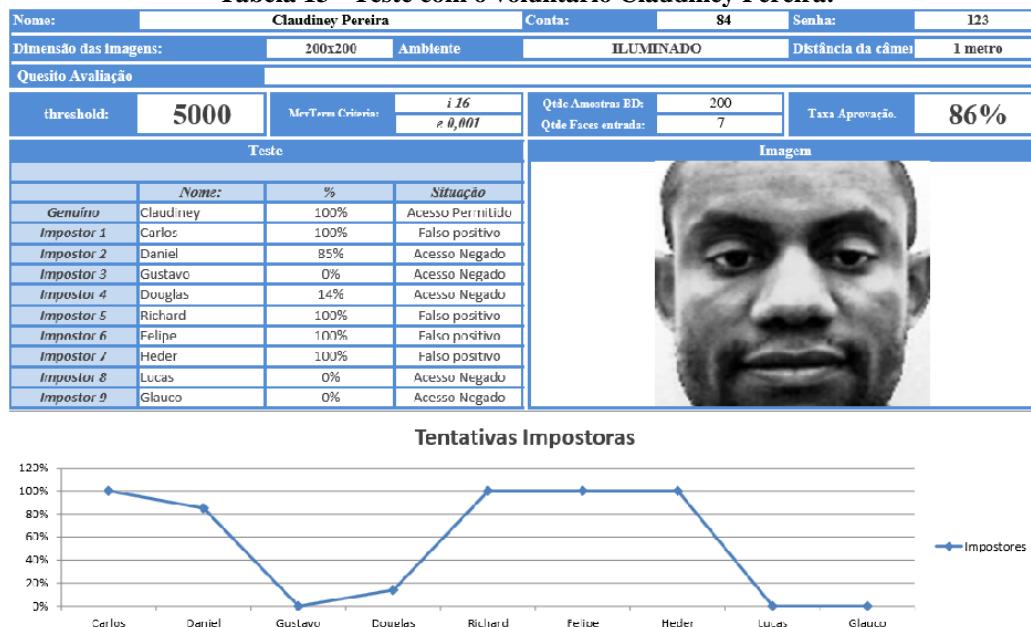
Na Tabela 11, teste realizado com o voluntário Daniel Simões. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 2 conseguiram acessar sua conta.

Tabela 11 - Teste com o voluntário Daniel Simões.

Na Tabela 12, teste realizado com o voluntário Carlos Piva. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 3 conseguiram acessar sua conta.

Tabela 12 - Teste com o voluntário Carlos Piva.

Na Tabela 13, teste realizado com o voluntário Claudiney Pereira. O mesmo foi autenticado com 100% de aprovação. Dos 9 impostores, apenas 3 conseguiram acessar sua conta.

Tabela 13 - Teste com o voluntário Claudiney Pereira.

Com os resultados demonstrados nas tabelas de coletas, verificamos que todos os genuínos fizeram acesso a suas respectivas contas com sucesso, todos com taxa de aprovação de 100%. Consequente a taxa de falsos negativos geradas é 0 (zero).

Com os impostores foram realizados 90 testes, sendo 9 impostores acessando cada uma das 10 contas. Dos 90 testes realizados com impostores tentando acessar contas alheias, 71 tiveram acesso negado, 78,90% do total. Resultando em 19 impostores com acesso permitido, o que gera uma taxa 21,10% de falsos positivos.

8.3. Testes Adicionais (Barba e Óculos)

Foram necessários testes adicionais para verificar o comportamento do protótipo em situações atípicas e que poderiam ocorrer no momento em que um cliente usa um caixa eletrônico, que é se o uso de algum acessório que possa atrapalhar a autenticação do cliente.

Os testes realizados foram: com uso de óculos, clientes cadastrados com barba e tentando acesso sem a mesma, e a tentativa de um impostor. Seguem na Tabela 14 e na Tabela 15 os resultados dos testes.

Na Tabela 14, constam os resultados de teste de acesso sem barba, com óculos e teste de tentativa de um impostor.

Tabela 14 - Testes com acessórios 1.

Nome:	Heder Lopes		Conta:	79	Senha:	123
Dimensão das imagens:	200x200		Ambiente	ILUMINADO		Distância da Cam: 1 metro
threshold:	5000	McvTerm Criteria:	i 16 e 0,001	Qtde Amostras BD: Qtde Faces entrada:	200 7	Taxa Aprovação.
Teste						
	s/Barba	Situação	Óculos	Situação	<i>Imagen</i>	
Teste 1	100%	Acesso permitido	100%	Acesso permitido		
Teste 2	100%	Acesso permitido	100%	Acesso permitido		
Teste 3	100%	Acesso permitido	100%	Acesso permitido		
Teste 4	100%	Acesso permitido	100%	Acesso permitido		
Teste 5	100%	Acesso permitido	100%	Acesso permitido		
	<i>Impostor</i>		<i>Situação</i>			
Teste 1	0%		Acesso Negado			
Teste 2	0%		Acesso Negado			
Teste 3	0%		Acesso Negado			
Teste 4	0%		Acesso Negado			
Teste 5	0%		Acesso Negado			

Da mesma forma na Tabela 15, foram realizados testes do cliente sem barba, um novo teste com óculos e a tentativa de um impostor.

Tabela 15 - Teste com acessórios 2.

Nome:	Richard Algarve	Conta:	91	Senha:	123
Dimensão das imagens:	200x200	Ambiente	ILUMINADO	Distância da Cam:	1 metro
threshold:	5000	McTerm Criteria:	i 16 e 0,001	Qtd Amostras BD: Qtd Faces entrada:	200 7
Teste					
s/Barba	Situação	Oculos	Situação	Imagen	
Teste 1	100%	Acesso permitido	100%	Acesso permitido	
Teste 2	100%	Acesso permitido	100%	Acesso permitido	
Teste 3	100%	Acesso permitido	100%	Acesso permitido	
Teste 4	100%	Acesso permitido	100%	Acesso permitido	
Teste 5	100%	Acesso permitido	100%	Acesso permitido	
Impostor		Situação			
Teste 1	0%		Acesso Negado		
Teste 2	0%		Acesso Negado		
Teste 3	0%		Acesso Negado		
Teste 4	0%		Acesso Negado		
Teste 5	0%		Acesso Negado		

Como detalhado em ambas as tabelas, 14 e 15, os resultados foram semelhantes. Para os testes de acesso sem barba e óculos, os resultados obtidos foram todos com 100% de aprovação o que consequentemente não gerou nenhuma taxa de falso negativo. Nas Figuras 36 e 37, podemos verificar a diferença entre imagens armazenadas e imagens utilizadas para comparação.



Figura 39 - Exemplo de comparação feita na tentativa de acesso.



Figura 40 - Segundo exemplo de comparação.

Para tentativa de acesso de impostores, em ambas as tabelas, em todos os testes seus acessos foram negados, o que não gerou nenhuma taxa de falso positivo.

8.4. Teste Adicional (Gêmeas)

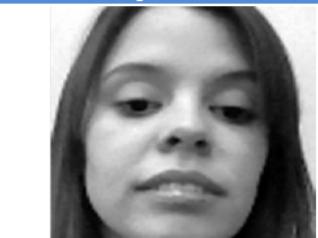
Na Tabela 16, estão demonstrados testes realizados com irmãs gêmeas idênticas. Neste primeiro teste, uma das gêmeas acessa sua conta normalmente, com 100% de aprovação. Com a tentativa de acesso da irmã, foi negado. Com isso nenhuma taxa de falso positivo ou falso negativo foi gerada.

Tabela 16 - Teste com gêmeas idênticas 1.

Nome:	Isabella Rocha		Conta:	Senha: 123	
Dimensão das imagens:	200x200		Ambiente	ILUMINADO	
threshold:	5000	McvTerm Criteria: <i>i 16 e 0,001</i>	Amostras BD: 200	Cam: 1 metro	Taxa Aprovação: 86%
			Faces entradas: 7		
Teste 1					Teste 2
<i>Genuína</i>	%		<i>Impostora</i>	%	
Isabella	100%		Nathalia	0%	
Isabella	100%		Nathalia	0%	
Isabella	100%		Nathalia	0%	
Isabella	100%		Nathalia	0%	
Isabella	100%		Nathalia	0%	
Imagen da Genuína			Imagen da Impostora		
					

Na Tabela 17, os testes foram invertidos. Os resultados obtidos foram os mesmos da Tabela 16. Nenhuma taxa de falso positivo ou falso negativo foi gerada.

Tabela 17 - Testes com gêmeas idênticas 2.

Nome:	Nathalia Rocha		Conta:	Senha: 123	
Dimensão das imagens:	200x200		Ambiente	ILUMINADO	
threshold:	5000	McvTerm Criteria: <i>i 16 e 0,001</i>	Amostras BD: 200	Cam: 1 metro	Taxa Aprovação: 86%
			Faces entradas: 7		
Teste 1					Teste 2
<i>Genuína</i>	%		<i>Impostora</i>	%	
Nathalia	100%		Isabella	0%	
Nathalia	100%		Isabella	0%	
Nathalia	100%		Isabella	0%	
Nathalia	100%		Isabella	0%	
Nathalia	100%		Isabella	0%	
Imagen da Genuína			Imagen da Impostora		
					

8.5. Verificação do tempo de detecção de face e do reconhecimento facial.

Foram realizados testes para verificar o tempo de detecção de uma face em uma imagem e o tempo que o protótipo leva para reconhecer e permitir o acesso do cliente ao menu de operações. Lembrando que no processo de reconhecimento compreende a detecção da face em uma imagem de entrada, a comparação da imagem de entrada com as imagens armazenadas durante o treinamento e a permissão do acesso.

- **Tempo de Detecção de face em uma imagem.**

Na Figura 41 é demonstrada uma amostra coletada do módulo administrativo do tempo que uma face é detectada em uma imagem.

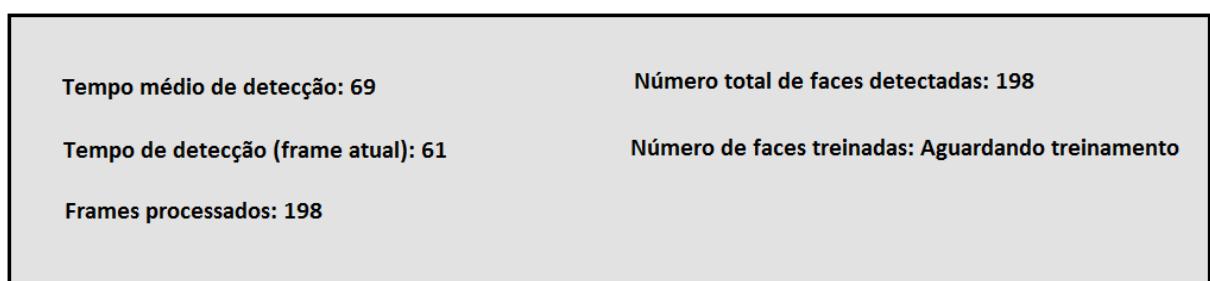


Figura 41 - Amostragem do tempo de detecção de uma face em uma imagem

Como nos mostra a Figura 41, no momento da coleta foram detectadas 198 faces com um tempo médio de 69 milésimos de segundos e a última face foi detectada em 61 milésimos de segundos.

- **Tempo de autenticação por meio do reconhecimento da face**

Para verificar o tempo que leva para um cliente ser reconhecido, foram coletadas amostras de 7 acessos ao módulo operacional. O tempo médio para cada acesso é de 630 milésimos de segundos e o tempo médio para fazer a comparação com cada imagem é de 90 milésimos de segundos. Os detalhes da amostragem estão demonstrados na Tabela 16:

Tabela 18 - Tempo médio para reconhecimento.

	Tempo/Acesso	Média/Acesso	Média/Imagem/Acesso	Média/Imagem
Acesso 1	619		88	
Acesso 2	636		91	
Acesso 3	643		92	
Acesso 4	636		91	
Acesso 5	621		89	
Acesso 6	719		103	
Acesso 7	536		77	

* Tempo em milésimos de segundos

9. CONCLUSÃO

Com bases em testes realizados com o protótipo *KeyFace* foram obtidos os dados os quais possibilitou verificar a viabilidade de implantação de um sistema de reconhecimento facial em um caixa eletrônico. No decorrer da pesquisa, verificou-se que para implantação de um sistema de reconhecimento facial, vários parâmetros devem ser considerados, pois em algumas situações em que o protótipo foi testado, não apresentou bons resultados, contudo, de forma geral, apresentou resultados satisfatórios.

A utilização do algoritmo de detecção facial Viola Jones, associado ao algoritmo *EigenFaces* (PCA), para verificação facial, apresentou resultados satisfatórios assim como dissertado no capítulo 8. A associação destes algoritmos apresentou baixa taxa de falsos positivos não gerando falsos negativos e foi satisfatória no que diz respeito a rotina de utilização de um caixa eletrônico, pois conforme objetivado nesta pesquisa, os tempos de processamento foram baixos, o que é de extrema importância em uma transação via caixa eletrônico, na qual geralmente os clientes estão aguardando em uma fila. Quanto a distância do cliente em relação a câmera, a solução atendeu perfeitamente, pois em caixas eletrônicos os clientes estão a menos de um metro do dispositivo de automação bancária.

Com a realização da pesquisa foram obtidas informações em diversas áreas do conhecimento servindo de base para a solução proposta e permitindo um embasamento sobre as fraudes que envolvem a utilização de um caixa eletrônico, como também os conceitos primordiais para os processos de reconhecimento facial. Na Tabela 19 a seguir é feita uma comparação entre pontos favoráveis e desfavoráveis para implantação.

Tabela 19 - Comparação dos pontos favoráveis e desfavoráveis.

Pontos favoráveis	Pontos desfavoráveis
<ul style="list-style-type: none"> • Apresentou baixos índices de TFP. • Não apresentou TFN. • Tempo de utilização favorável. • Distância favorável. • Permitiu distinção de gêmeos idênticos. • Descaracterizações faciais foram aceitas. • Permite gerar histórico facial de acessos. 	<ul style="list-style-type: none"> • Parâmetros ajustados por ambiente. • Funcional em ambiente iluminado. • Instabilidade no reconhecimento devido à posição do usuário. • Pode ser burlado por imagens faciais estáticas. • Não trata explosões e assaltos (internos e externos).

Ao geral, a solução proposta é viável para utilização em caixas eletrônicos e tende a deixar de ser mera ficção para ser adotada no mundo real. Os sistemas de segurança devem estar preparados para se adequarem a uma realidade cada vez mais perigosa onde o reconhecimento facial pode ser a solução para controles de acesso.

9.1. Implementações Futuras

- Detectar fraudes provenientes de uma falsa face (faces provenientes de fotos). Pode haver a possibilidade de um indivíduo apresentar uma imagem estática (foto) com o intuito de burlar o sistema. Evitar a captura de fotos pode ser implantado como melhoria
- Aperfeiçoar o algoritmo evitando TFP e TFN e se necessário adotar outro algoritmo de extração de características para melhores resultados.
- Desenvolver um algoritmo de classificação externo a implementação fornecida com o framework.
- Buscar redução no número de amostras mantendo a precisão com menores índices de TFP e TFN.
- Através da detecção facial desenvolver uma câmera móvel que localize uma face a frente do caixa eletrônico independendo da altura do indivíduo

REFERÊNCIAS

A3M. Cartões magnéticos, Cartão plástico com banda magnética para gravar dados. Disponível em:<<http://www.a3m.eu/pt/cartoes-plasticos/cartoes-brancos/Cartoes-magneticos>>. Acesso em: 06 março 2014.

ACESSO E PONTO. Biometria, a chave é você. Informações sobre uso de tecnologia de acesso e ponto eletrônico. Disponível em: <<Http://acessoeponto.mixlog.com.br/tag/identificacao-retina/>> Acesso em: 18 abril 2014.

AMORIM, Paulo Roberto Figueiroa. Biometria. Centro de Informática. Universidade Federal de Pernambuco. Recife, 19 Dezembro 2005.

ARISP. Certificados Digitais, O que é um Certificado Digital? O que é um *Smart Card*? Disponível em: <http://www.ar.arisp.com.br/conteudo/faq_cnpj.htm>. Acesso em: 29 março 2014.

BEYMER, David; **POGGI,** Tomasio. “Face Recognition from One Example View”, Massachusetts Institute of technology – MTI. Artificial Intelligence Laboratory, 1995.

BONATO, Cassiana da Silva. **NETO,** Roberto Mendes Finzi. Um Breve Estudo Sobre Biometria. Departamento de Ciência da Computação – Universidade Federal de Goiás (UFG) – Campus Catalão. Catalão, Goiás. 2010.

BRAGA, Marco Aurélio. Um jeito sofisticado para clonar cartões. A Notícia. Disponível em: Joinville, SC. 28 junho 2007. Disponível em:<<http://www.an.com.br/2007/jun/28/0pol.jsp>>. Acesso em: 26 março 2014.

BRASIL. Superior tribunal de justiça. Mesmo sem culpa, banco tem que indenizar vítimas de fraudes cometidas por terceiros. Recurso Repetitivo. Brasília. 29 agosto 2011. Disponível em:<http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=102986> Acesso em: 09 março 2014.

CABRAL, Gabriela. Biometria, Portal R7 Educação, Disponível em:<<Http://www.brasilescola.com/informatica/biometria.htm>>. Acesso em: 16 abril 2014.

CARDCOM. Como conservar seu cartão. Belo Horizonte. Disponível em:<<Http://www.cardcom.com.br/como-conservar-seu-cartao/>>. Acesso em: 23 março 14.

CBA (Consultores Biométricos Associados). Como a Biometria funciona. O Procedimento. Empresa de consultoria especializada em biometria aplicada, nas áreas de segurança física, lógica, identificação civil e criminal.<http://www.consultoresbiometricos.com.br/05_Cbio_funciona.php> 18 abril 2014.

CEPSRM (Centro Estadual de Pesquisas em Sensoriamento remoto e meteorologia). Página Dinâmica para Aprendizado do Sensoriamento Remoto. Universidade Federal do Rio Grande do Sul Disponível em: <<http://www.ufrgs.br/engcart/PDASR/hist.html#2>>. Acesso em: 30 setembro 2014.

CERIGATTO, Mariana. Golpe da ‘troca de cartões’ visa idosos. Jornal da Cidade. Bauru. 03 março 2014. Disponível m:<<http://www.jcnet.com.br/Policia/2011/05/golpe-da-troca-de-cartoes-visa-idosos.html>>. Acesso em: 25 março 2014.

CIDADE VERDE. Economia, Um em cada quatro usuários de cartões já sofreram alguma fraude. TV Cidade Verde. Teresina, PI. 24 novembro 2012, Disponível em:<<http://www.cidadeverde.com/brasil-ocupa-7-lugar-em-ranking-de-fraudes-com-cartoes-diz-pesquisa-118869>>. Acesso em: 24 março 2014.

DEPARTAMENTO DE INFORMATICA DA UNIVERSIDADE FEDERAL DO PERNABUCO. Equalização do Histograma. Disponível em: <http://www.di.ufpe.br/~if143/projetos/99_2/equali/Equalizacao.html>. Acesso em 06 outubro 2014.

DEPARTAMENTO DE POLÍCIA FEDERAL. Operações, Resumo de operações DPF – 2007. Disponível em: <http://www.dpf.gov.br/agencia/estatisticas/2007#Pen_drive> Acesso em: 26 março 2014.

DINIZ, Fábio Abrantes, **NETO**, Francisco Milton Mendes, **LIMA**, Francisco das Chagas Júnior, **FONTES**, Laysa Mabel de O..*RedFace*: um sistema de reconhecimento facial baseado em técnicas de Análise de componentes principais e auto faces: comparação com diferentes classificadores. Programa de Pós-Graduação em Ciência da Computação, UERN/UFERSA, Campus Central, Mossoró, RN, Revista Brasileira de Computação Aplicada (ISSN 2176-6649), Passo Fundo, v. 5, n. 1, p. 42-54, abr. 2013.

EMGUVC. Main Page. Disponível em: <http://www.emgu.com/wiki/index.php/Main_Page>. Acesso em: 20 abril 2014.

ESTADÃO. Cartão: bancos substituem tarja magnética por chip. 5 março 2002. Disponível em: <[Http://www.estadao.com.br/arquivo/economia/2002/not20020305p9162.htm](http://www.estadao.com.br/arquivo/economia/2002/not20020305p9162.htm)> Acesso em: 29 março 2014.

FARINA, André Marcelo. BIOMOBILE: Sistema de Identificação de Usuários em Dispositivos Móveis na Plataforma Android Utilizando Reconhecimento de Faces a Partir de Vídeo. Dissertação apresentada para obtenção do título de Mestre em Ciência da Computação, área de Processamento de Imagens e Visão Computacional, junto ao Programa Pós-Graduação em Ciência da Computação. UNIVERSIDADE ESTADUAL PAULISTA-UNESP. Bauru, 2012.

FEBRABAN (Federação Brasileira de Bancos). A responsabilidade é dos bancos. São Paulo. 2008. Disponível em:< http://www.febraban.org.br/Febraban.asp?id_pagina=124&id_paginaDe=121>. Acesso em: 26 março 2014.

FREITAS, Aiana. Especialistas dão 7 dicas para consumidor que sofre fraude no cartão.Portal UOL, em São Paulo 09 maio 2013. Disponível em:<<http://economia.uol.com.br/noticias/redacao/2013/05/09/especialistas-dao-7-dicas-para-consumidor-que-sofre-fraude-no-cartao.htm>>. Acesso em: 26 março 2014.

G1 DSITRITO FEDERAL. Polícia realiza ação contra esquema de fraude em cartão de crédito no DF. Distrito Federal. 21 janeiro 2014. Disponível em: <<http://g1.globo.com/distrito-federal/noticia/2014/01/policia-realiza-acao-contra-esquema-de-fraude-em-cartao-de-credito-no-df.html>> Acesso em: 25 março 2014.

G1 RIO. Correntistas têm fatura do cartão de crédito falsificada em boletos no Rio. Globo.com. Rio de janeiro 19 março 2014. Disponível em:<http://g1.globo.com/rio-de-janeiro/noticia/2014/03/correntistas-tem-fatura-do-cartao-de-credito-falsificada-em-boletos-no-rio.html> >. Acesso em: 31 março 2014.

G1 GOIÁS. Presos três suspeitos de fraudar caixas eletrônicos em GO, Rio e SP.Globo.com. Goiânia. 10 junho 2013. Disponível em:<<http://g1.globo.com/goias/noticia/2013/06/presos-tres-suspeitos-de-fraudar-caixas-eletronicos-em-go-rio-e-sp.html>>. Acesso em: 01 abril 2014.

GARCIA, Iberê Anselmo. A segurança na identificação: A biometria da íris e da retina. Faculdade de Direito da Universidade de São Paulo-USP. São Paulo. 2009.

JORNAL NACIONAL. Clonagem de cartões no Brasil aumenta quase 50%. Portal Globo.com. 06 agosto 2009. Disponível <<http://jornalnacional.globo.com/Telejornais/JN/0,,MUL1257829-10406,00-CCLONAGEM+DE+CARTOES+NO+BRASIL+AUMENTA+QUASE.html>>Acesso em: 09 março 2014.

GONZALEZ, Rafael C.;**WOODS,** Richard E.; Processamento de imagens digitais. São Paulo. Ed. Edgard Blücher. 1992.

GUSMÃO, Gustavo. Windows XP está presente em 95% dos caixas eletrônicos pelo mundo. INFO .Online . Editora Abril S.A..20 janeiro 2014. Disponível em:<<http://info.abril.com.br/noticias/ti/2014/01/windows-xp-esta-presente-em-95-dos-caixas-eletronicos-pelo-mundo.shtml>> Acesso em: 29 março 2014.

IBIOMÉTRICA. Biometria - Centro de Conhecimento, Tipo de dados biométricos <http://www.Ibiometrica.com.br/biometria_sistemas.asp> 18 abril 2014.

INSPER (instituto de ensino e pesquisa),**CPP** (Centro de políticas públicas). Relatório da Pesquisa de Vitimização em São Paulo. São Paulo. 2013. Disponível em:<<http://estaticog1.globo.com/2013/10/22/Relatorio-de-Vitimizacao-ok-2013-v6.pdf>> Acesso em: 09 março 2014.

ITAÚ, banco. Com biometria, cliente Itaú pode sacar sem uso do cartão. Imprensa. 18 dezembro 2012. Disponível em: <<https://www.itau.com.br/imprensa/releases/com-biometria-cliente-itau-pode-sacar-sem-uso-do-cartao.html>

JAIN, Anil, **HONG,** Lin, **PANKANTI,** Sharath, **BOLLE,** Ruud. An Identity Authentication System Using Fingerprints. Department of Computer Science Michigan State University East Lansing, MI 48824 And Exploratory Computer Vision Group IBM T. J. Watson Research Center Yorktown Heights, NY 10598. 1997.

JAIN, Anil K., **ROSS**, Arun, **PRABHAKAR** Salil. *An Introduction to Biometric Recognition*. Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

JORNAL NACIONAL. Clonagem de cartões preocupa consumidores. Globo.com. 03 fevereiro 2010. Disponível em:<<http://jornalnacional.globo.com/Telejornais/JN/0,,MUL1475832-10406,00-CLONAGEM+DE+CARTOES+PREOCUPA+CONSUMIDORES.html>> Acesso em: 28 março 2014.

JUSTE, Marília. Região nobre do cérebro é capaz de ‘prever’ quando verá uma face. Portal G1. São Paulo. 23 novembro 2006. Disponível em:<<http://g1.globo.com/Noticias/Ciencia/0,,AA1361786-5603,00.html>> Acesso em: 04 março 2014.

KINUTA, Cristiane, **MOLINA**, Dennis, **DORNELES**, Eric Giovanni, **GRECCHI**, Fabio Simeão, **DIAS**, Gilson Torres, **SANTANA**, Jailton, **JUNIOR**, Oswaldo Ortiz Fernandes. Estudo comparativo para reconhecimento facial. Universidade IMES - São Caetano do Sul – SP, 2013.

KIRBY, M., **SIROVICH**, L.. Application of the Karhunen-Lokve Procedure for the Characterization of Human Faces .1 janeiro 1990.

LI, Stan Z., **JAIN**, Anil K.. Handbook of face recognition. Editora Springer, New York, NY, EUA, 2005.

LOPES, Eduardo Costa. Detecção de Faces e Características faciais.Trabalho Individual II de Pós-Graduação em Ciência da Computação.Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) Porto Alegre. Disponível em: <www3.pucrs.br/pucrs/files/uni/poa/facin/pos/relatoriostec/tr045.pdf> Acesso em: 08 março 2014.

LORDELLO, Jorge. Arapuca caixas eletrônicos 24h.Tudo sobre segurança. 09 Março 2014. Disponível em:<http://tudosobreseguranca.com.br/portal/index.php?option=com_content&task=view&id=233&Itemid=152> Acesso em: 09 março 2014.

MARTINS, Júlio. Parâmetros da imagem no domínio digital: o que é pixel, resolução de imagem, resolução de captura e outras características da imagem digital ou digitalizada. Disponível em: <http://www.novomilenio.br/comunicacoes/1/artigo/12_julio_martins.pdf>, Acesso em: 30 setembro 2014.

MEDEIROS, Luciano Xavier. Reconhecimento facial utilizando análise de componentes principais e algoritmo genético em imagens segmentadas. 2012. Tese de Doutorado. Faculdade de Engenharia Elétrica da Universidade Federal de Uberlândia. Uberlândia 2012.

MELLO, Carlos Alexandre. Limiarização. Pós-Graduação em Ciência da Computação, Centro de informática da UFPE (Universidade Federal de Pernambuco). Disponível em:<http://www.cin.ufpe.br/~cabm/visao/Aula04_Limiarizacao.pdf>. Acesso em: 30 setembro 2014.

MILANO, Danilo de, **HONORATO**, Luciano Barrozo. Visão Computacional UNICAMP – Universidade Estadual de Campinas FT – Faculdade de Tecnologia. Disponível em: <http://www.ft.unicamp.br/liag/wp/monografias/monografias/2010_IA_FT_UNICAMP_visa_oComputacional.pdf>. Acesso em: 01 outubro 2014.

MINORITY REPORT, A nova lei. Produção de Bonnie Curtis, Gerald R. Molen. Direção de Steven Spielberg. Roteiro de Frank Darabont, Gary Goldman, John August, Jon Cohen, Ronald Shusett, Scott Frank. Fotografia de Janusz Kaminski. Trilha Sonora de John Williams. Elenco: Colin Farrell, Kathryn Morris, Max von Sydow, Peter Stormare, Samantha Morton, Tom Cruise. EUA. 2002. (145 min). Sonoro. Color. Legendado. Port.

MONITOR DAS FRAUDES. Cartilha de segurança, Introdução a finalidade dos ataques. 22 fevereiro 2014. Disponível em: <<http://www.fraudes.org/showpage1.asp?pg=110>>. Acesso em: 28 março 2014.

MUNDO ESTRANHO. Como funcionam os caixas eletrônicos?, Tecnologia. Revista eletrônica, Editora Abril. 2012. Disponível em: <<http://mundoestranho.abril.com.br/materia/como-funcionam-os-caixas-eletronicos>>. Acesso em: 12 março 2014.

NEMES, Ana, Fotografia: como funcionam os histogramas. Portal Tech Mundo. 17 fevereiro 2011. Disponível em: <<http://www.tecmundo.com.br/8616-fotografia-como-funcionam-os-histogramas.htm>>. Acesso em: 30 setembro 2014.

NOCELLI, Gracielle. Brasil caminha para ser referência na biometria em bancos. Tribuna de Minas. Juiz de Fora, MG. 24 janeiro 2014. Disponível em: <<http://www.tribunademinas.com.br/economia/brasil-caminha-para-ser-referencia-na-biometria-em-bancos-1.1416652>>. Acesso em: 27 março 2014.

O GLOBO. Operação Pen Drive: total de 17 pessoas presas por clonagem de cartão. GLOBO ONLINE. 28 junho 2007. Disponível em: <<http://oglobo.globo.com/economia/operacao-pen-drive-total-de-17-pessoas-presas-por-clonagem-de-cartao-4178491>>. Acesso em: 26 março 2014.

OPENCV. About. Disponível em: <<http://opencv.org/about.html>>. Acesso em: 20 abril 2014.

OPENCV DOCUMENTATION. OpenCV 2.4.9.0 documentation . Disponível em: <<http://docs.opencv.org/>>. Acesso em: 20 abril 2014.

OTAVIANO, Christopher Henrique. Biometria: Seus métodos e aplicações. Curso de Ciência da Computação, Universidade Estadual de Mato Grosso do Sul. Dourados – MS, 2005.

PENTEADO, Bruno Elias. Autenticação de usuários em sistemas de e-learning baseada em reconhecimento de faces a partir de vídeo. Dissertação apresentada para obtenção do título de Mestre em Ciência da Computação, área de Processamento de Imagens e Visão Computacional, junto ao Programa Pós- Graduação em Ciência da Computação. UNIVERSIDADE ESTADUAL PAULISTA- UNESP. Bauru, 2009.

PEREIRA, Milena. "Facebook melhora reconhecimento facial e chega quase ao nível humano". TechTudo. Disponível em: <<http://www.techtudo.com.br/noticias/noticia/2014/03/facebook-melhora-reconhecimento-facial-e-chega-quase-ao-nivel-humano.html>>. Acesso em: 18 março 2014.

PORTAL G1. Bando clona milhares de cartões com chip. Do G1, com informações do SPTV. 30 junho 2007. Disponível em:<<http://g1.globo.com/Noticias/SaoPaulo/0,,MUL61618-5605,00.html>>. 26 março 2014.

QUECONCEITO, Dicionário online de Conceitos. Conceito de segurança. Disponível em: <<http://queconceito.com.br/seguranca#ixzz2uCKRr5dH>> Acesso em: 09 março 2014.

ROHR, Altieres. Vírus brasileiro adapta ataque do 'chupa cabra' em máquinas de cartão.G1 Tecnologia e games. Portal Globo.com. 10 fevereiro 2012. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2012/02/virus-brasileiro-adapta-ataque-do-chupa-cabra-em-maquinhas-de-cartao.html>>. Acesso em: 25 março 2014.

SERVIÇO BANCÁRIOS. O que é um caixa automático. 18 setembro 2010. Disponível em:<<http://www.servicosbancarios.com.br/2010/09/o-que-e-um-caixa-automatico-atm.html>> Acesso em: 29 março 2014.

SILVA, Clevertom, **MIRANDA**, Daiana de, **OLIVEIRA**, Fabiana de, **FERREIRA**, Júlio Cesar, **FALBO** Leandro, **SILVEIRA**, Pedro Sérgio. A Segurança através da Biometria. Simpósio de Excelência em Gestão e Tecnologia, 4, 2007. Anais... Resende: Associação Educacional Dom Bosco, 2007. P.2.

SILVA, Antônio Machado e. Curso Processamento digital de imagens de satélite. Centro de Eventos da PUCRS - de 07 a 12 de outubro de 2001. Porto Alegre - RS. Disponível em <www.cartografia.org.br>. Acesso em: 19 fev. 2007.

SLAIBI CONTI, M.. A BIOMETRIA E A SEGURANÇA DE DADOS. Revista de Estudos Jurídicos, América do Norte, 0, abr. 2012. Disponível em:<<http://revista.universo.edu.br/index.php?journal=4pesquisa3&page=article&op=view&path%5B%5D=529&path%5B%5D=367>>. Acesso em: 16 Abril 2014.

TELECO. Sistemas de Edição para TV I: Imagens e Sinais. Disponível em: http://www.teleco.com.br/tutoriais/tutorialsedtv/pagina_2.asp. Acesso em: 19 abril 2014.

TSE (Tribunal Superior de Eleitoral). Biometria, Apresentação. Brasília. 19 julho 2013. Disponível em: <<http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/biometria-1>> Acesso em: 21 abril 2014.

TURK, Matthew, **PENTLAND**, Alex. *Eigenfaces for Recognition. Journal of Cognitive Neuroscience*. Massachusetts Institute of Technology. Volume 3 Number 1. 1991.

VEJA ONLINE. Sua segurança, Seus dados valem ouro. Editora Abril S.A. 13 junho 2001. Disponível em: <http://veja.abril.com.br/especiais/seguranca/p_092.html> Acesso em: 23 fevereiro 2014.

VIOLA, Paul, **JONES**, Michael. Rapid Object Detection using a Boosted Cascade of Simple Features. ACCEPTED CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION, 2001.

ZENICOLA BRAGA, Luiz Felipe. Sistemas de reconhecimento facial. Trabalho de Conclusão de Curso apresentado a Escola de Engenharia de São Carlos da Universidade de São Paulo. Curso de Engenharia Elétrica com ênfase em Eletrônica. São Carlos, 2013.

ZHAO, W.; **CHELLAPPA**, R.; **PHILLIPS**, P. J.; **ROSENFELD**, A. Face recognition: A literature survey. ACM Computing Surveys. 2003.

ZMOGISNKI, Felipe. Operação Pen drive e o cracker que fraudou o *smart card*. Info Online Editora Abril. São Paulo. 02 julho 2007. Disponível em: <<http://info.abril.com.br/aberto/infonews/072007/02072007-8.shl>> Acesso em: 09 março 2014.

APÊNDICES

APÊNDICE A - Termos de autorização de uso de Imagem

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Felipe Cardoso Almeida Costa, nacionalidade brasileiro, estado civil Solteiro, portador da Cédula de identidade RG nº. 36280395-2, inscrito no CPF/MF sob nº 390524978-26, residente à Avenida/Rua Estevam Maturano Alcarreto, nº. 1502, Complemento Corte município Pederneiras

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneira, dia 26 de agosto de 2014.

FPCosta
(assinatura)

Nome: Felipe Costa

Telefone p/ contato: (17) 991269592

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Jáuio Guilherme Gallardo, nacionalidade Branidente,
 estado civil Solteiro, portador da Cédula de identidade RG nº. 44.570.648-2C, inscrito
 no CPF/MF sob nº 439.307.498-07, residente à Av/Rua
Av. João Lemos, nº.
360, Complemento município Banini - SP

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Paertree - FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/ SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 10 de novembro de 2014.

Jáuio G Gallardo
 (assinatura)

Nome:

Telefone p/ contato:

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Daniel Coque Simões, nacionalidade Brasileira, estado civil Solteiro, portador da Cédula de identidade RG nº 34036800-7, inscrito no CPF/MF sob nº 324.929.978-58, residente à Avenida/Rua Fausto Furlani, nº 1100, Complemento OESTE município Pederneiras

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 08 de Agosto de 2014.

Daniel C. Simões
(assinatura)

Nome: Daniel Coque Simões

Telefone p/ contato: (14) 996936263

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Douglas Rafael Gennaro, nacionalidade Brasileiro, estado civil Solteiro, portador da Cédula de identidade RG nº. 46.577.232-6 inscrito no CPF/MF sob nº 223.099.748-70, residente à Avenida/Rua Abelicas, Centro, nº. 66, Complemento _____ município Mogi das Cruzes

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcams, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 26 de Agosto de 2014.

Douglas R. Gennaro.
(Assinatura)

Nome: Douglas Rafael Gennaro.

Telefone p/ contato: (14) 99725 0906

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Carlos Roberto Lira Junio, nacionalidade Brasileiro, estado civil Solteiro, portador da Cédula de identidade RG nº. 42.293.507-5, inscrito no CPF/MF sob nº 337.421.968-76, residente à Avenida/Rua Ary Barroso 02775, Complemento _____, município Pedreira, nº.

São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pedreira, dia 26 de Agosto de 2014.

 (assinatura)

Nome: Carlos Roberto Lira Junio

Telefone p/ contato:

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Gustavo Lulinio de Almeida, nacionalidade Brasileiro estado civil Solteiro, portador da Cédula de identidade RG nº 45037987-2, inscrito no CPF/MF sob nº 41298838878, residente à Avenida/Rua Estevam Moturama Alcâncar, nº. 1519, Complemento Oeste município Pederneiras

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartrec- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855. Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 26 de Agosto de 2014.

(assinatura) Gustavo

Nome: Gustavo Lulinio de Almeida

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, CLAUDINÉY P. DA SILVA, nacionalidade BRASILEIRO, estado civil CASADO, portador da Cédula de identidade RG nº 10502213, inscrito no CPF/MF sob nº 039.709.826-00, residente à Avenida/Rua ANTONIO PORCINO FILHO, nº. 68, Complemento _____ município ALVORADA

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

PEDERNEIRAS, dia 12 de AGOSTO de 2014.

(assinatura)

Nome: CLAUDINÉY P. SILVA

Telefone p/ contato: (14) 98804-9127

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Isabellla da Rocio Acosta, nacionalidade Brasileira,
 estado civil solteira, portador da Cédula de identidade RG nº 34.384.851-0, inscrito
 no CPF/MF sob nº 422.895.678-50, residente à Avenida/Rua
Rinchuelo 96, Complemento Oeste município Pederneiras

São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 27 de Agosto de 2014.

Isabellla
 (assinatura)

Nome: Isabellla

Telefone p/ contato: 9-9174-5240

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Notácia da Rocha Acosta, nacionalidade _____, estado civil solutivo, portador da Cédula de identidade RG nº 34384856 - 9, inscrito no CPF/MF sob nº 422 895 668-88, residente à Avenida/Rua Pedreira, nº. 86, Complemento Oeste município Pederneiras

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pederneiras/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pederneiras, dia 27 de agosto de 2014.

Notácia da Rocha Acosta
(assinatura)

Nome:

Telefone p/ contato: (14) 99616-4044

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM

Neste ato, Lucas Beltrão Sgo, nacionalidade Brasileiro,
 estado civil Solteiro, portador da Cédula de identidade RG nº. 40396173-7, inscrito
 no CPF/MF sob nº 419.832.338-03, residente à Avenida/Rua
Silviano 200, 17, Vila 509 Silviano, nº.
Coxa município Foxá - SP

/São Paulo. AUTORIZO o uso de minha imagem, para ser utilizada em testes do Trabalho de Conclusão do curso de Sistemas de Informação, "Reconhecimento Facial voltado à segurança de caixas eletrônicos", da Faculdade Gennari & Peartree- FGP, com sede no Parque Colina Verde, Rua Prof. Massud José Nacher, 2855, Pedreira/SP, sejam essas destinadas apenas para fins acadêmicos. A presente autorização é concedida a título gratuito, abrangendo o uso da imagem acima mencionada no perímetro da faculdade citada, da seguinte forma: (I) Coleta de amostras de Faces via webcam, armazenadas em banco de dados, para verificação do funcionamento do protótipo capaz de fazer a verificação de um indivíduo pela face. Por esta ser a expressão da minha vontade declaro que autorizo o uso acima descrito sem que nada haja a ser reclamado a título de direitos conexos à minha imagem ou a qualquer outro, e assino a presente autorização em 02 vias de igual teor e forma.

Pedreira, dia 26 de Agosto de 2014.

lucsb6.
 (assinatura)

Nome: Lucas Beltrão Sgo
 Telefone p/ contato: (14) 99794-8826