**FACULDADE DE TECNOLOGIA DE SÃO JOSÉ DOS CAMPOS**

**FATEC PROFESSOR Jessen Vidal**

**samara cardoso dos santos**

**PESQUISA E DESENVOLVIMENTO DAS PRINCIPAIS TÉCNICAS E MÉTODOS PARA CONTROLE DE ACESSO UTILIZANDO RECONHECIMENTO DE PADRÕES BIOMÉTRICOS PARA INTERNET**

São José dos Campos

2015

**samara cardoso dos santos**

**PESQUISA E DESENVOLVIMENTO DAS PRINCIPAIS TÉCNICAS E MÉTODOS PARA CONTROLE DE ACESSO UTILIZANDO RECONHECIMENTO DE PADRÕES BIOMÉTRICOS PARA INTERNET**

Trabalho de Graduação apresentado à Faculdade de Tecnologia São José dos Campos, como parte dos requisitos necessários para a obtenção do título de Tecnólogo em Informática com Ênfase em Análise e Desenvolvimento de Sistemas.

**Orientador: Me. Diogo Branquinho Ramos**

**Co-Orientador: Diego Palharini**

São José dos Campos

2015

SOBRENOME, Nome do Aluno

Título do Trabalho de Graduação.

São José dos Campos, 200X.

999f. (número total de folhas do TG)

Trabalho de Graduação – Curso de Tecnologia em (Logística, Informática ou Aeronáutica) com

Ênfase em Xxxxxxx, FATEC de São José dos Campos: Professor Jessen Vidal, 20XX.

Orientador: Titulação Nome do Orientador.

1. Áreas de conhecimento. I. Faculdade de Tecnologia. FATEC de São José dos Campos: Professor Jessen Vidal. Divisão de Informação e Documentação. II. Título

**REFERÊNCIA BIBLIOGRÁFICA –**

SOBRENOME, Nome do Aluno. **Título do Trabalho de Graduação.** 20XX. 999f. Trabalho de Graduação - FATEC de São José dos Campos: Professor Jessen Vidal.

**CESSÃO DE DIREITOS –**

NOME DO AUTOR: Nome do Aluno

TÍTULO DO TRABALHO: Título do Trabalho de Graduação

TIPO DO TRABALHO/ANO: Trabalho de Graduação / 20XX.

É concedida à FATEC de São José dos Campos: Professor Jessen Vidal permissão para reproduzir cópias deste Trabalho e para emprestar ou vender cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte deste Trabalho pode ser reproduzida sem a autorização do autor.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome do Aluno

Endereço do Aluno

CEP XXX-XX – Cidade - Estado

**samara cardoso dos santos**

**PESQUISA E DESENVOLVIMENTO DAS PRINCIPAIS TÉCNICAS E MÉTODOS PARA CONTROLE DE ACESSO UTILIZANDO RECONHECIMENTO DE PADRÕES BIOMÉTRICOS PARA INTERNET**

Trabalho de Graduação apresentado à Faculdade de Tecnologia São José dos Campos, como parte dos requisitos necessários para a obtenção do título de Tecnólogo em Informática com Ênfase em Análise e Desenvolvimento de Sistemas.

**Composição da Banca**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Nome do Componente da Banca, titulação e Instituição**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Nome do Componente da Banca, titulação e Instituição**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Nome do Orientador, titulação e Instituição**

**\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_**

**DATA DA APROVAÇÃO**

**Agradecimentos**

**Resumo**

**ABSTRACT**

**LISTA DE figuras**

[**Figura 1- Uso da Biometria** 13](#_Toc424762287)

[**Figura 2- Fases para processo de reconhecimento do padrão biométrico** 17](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762288)

[**Figura 3 - Segurança da Informação: Tríade CIA** 18](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762289)

[**Figura 4 - Processo de criptografia simétrica** 20](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762290)

[**Figura 5 - Processo de criptografia assimétrica** 21](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762291)

[**Figura 6 - Métodos de Biométricos** 23](#_Toc424762292)

[**Figura 7- Requisitos dos Sistemas Biométricos** 24](#_Toc424762293)

[**Figura 8 - Tipo de características biométricas** 25](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762294)

[**Figura 9 - Processo de reconhecimento da Íris adaptado de** (JAIN, 2011)**.** 26](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762295)

[**Figura 10 - Vista lateral da retina** 27](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762296)

[**Figura 11 - Processo de reconhecimento da impressão digital** 29](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762297)

[**Figura 12- Principais linhas e rugas da mão** 30](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762298)

[**Figura 13- Sistema de verificação de assinatura on-line** 31](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762299)

[Figura 14- Representação da obtenção das DoG para as oitavas de uma imagem 36](file:///C:\Users\Samara%20Cardoso\Desktop\TG-%20Samara.docx#_Toc424762300)

**LISTA DE tabelas**

[**Tabela 1 - Comparação das características biométricas mais utilizadas** 27](#_Toc424762356)

**LISTA DE abreviaturas e siglas**

**Sumário**

[1. INTRODUÇÃO 13](#_Toc425097850)

[2. REVISÃO BIBLIOGRÁFICA 19](#_Toc425097855)

[3. DESENVOLVIMENTo 35](#_Toc425097859)

[4. RESULTADO 39](#_Toc425097860)

[5. CONSIDERAÇÕES FINAIS 39](#_Toc425097861)

[6. REFERÊNCIAS 39](#_Toc425097862)

1. **INTRODUÇÃO**
2. **CONTEXTO**

Os avanços científicos e tecnológicos dos últimos anos provocou um aumento significativo por produtos e serviços baseados em tecnologia, principalmente os que estão relacionados com telecomunicações, informática, etc. Em função disso é necessário ter segurança nas informações no sentido de preservar o valor em que elas possuem para um indivíduo ou para uma organização.

A segurança em sistemas de informação faz-se necessária para a sobrevivência de qualquer empresa. Possuir um sistema com segurança é algo de valor significativo, contudo, o perigo de um ataque não é ignorado totalmente. Neste contexto, a segurança da informação deve ser tomada como opção estratégica e não apenas, com impacto positivo e inegável sobre o negócio.

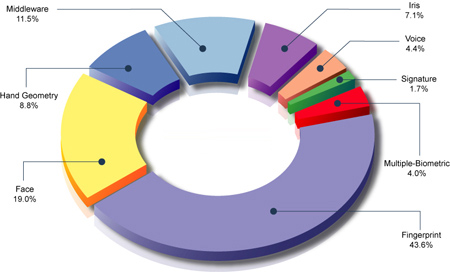
Desta forma, tornar um sistema informação seguro é uma tarefa que necessita conhecimento e habilidade para detectar rapidamente as ameaças, antes que estas se transformem em ataques e criem problemas que tornem os sistemas inoperantes, causando sérios transtornos para seus usuários. (PINHEIRO, 2008).

Tradicionalmente, as senhas e cartões de identificação são usados para restringir o acesso a sistemas de informação. No entanto, a segurança pode ser facilmente violada, pois nestes sistemas a senha pode ser revelada ou um cartão de autorização de acesso pode ser roubado. Além disso, senhas simples são fáceis de adivinhar e senhas difíceis podem ser complicadas de serem lembradas pelo o usuário. A Biometria é uma das mais avançadas tecnologias de segurança, que identifica pessoas conforme padrões biométricos: características físicas e únicas de cada indivíduo. (BARROS, GOMES e FREITA, 2011).

A palavra biometria vem do grego: *bios* (vida) e *metron* (medida) o estudo das características biológicas (anatômicas e fisiológicas) ou comportamentais mensuráveis dos seres vivos, de forma estatística, analisando os padrões e os definindo em atributos quantitativos para a identificação de um indivíduo. A impressão digital, o DNA, íris, padrões de voz, impressões palmares e padrões faciais, são algumas das características que tornam cada ser humano único, possibilitando assim o desenvolvimento de diversas aplicações para reconhecimento e identificação desses padrões. (NSTC, 2006).

Atualmente estudos vêm sendo realizados para possibilitar a utilização da Biometria em várias áreas, ajudando em diferentes tarefas. Isto atende desde o usuário simples até um sistema de segurança e identificação de criminosos. (PEREIRA, REZENDE, *et al.*, 2007). A Figura *1* mostra com base em estatística de pesquisa da *International Biometrics Group (IBG)* o uso da biometria como uma maneira de identificação humana.

**Figura 1- Uso da Biometria**



**Fonte: IBG, 2009.**

A biometria está presente na emissão de visto, controle de fronteira, carteiras de habilitação, trabalho, etc. A vantagem do uso da biometria é que o usuário não necessita levar consigo cartões de autenticação e nem tão pouco se lembrar de senhas. Outro ponto que deve ser analisado é que uma característica biométrica não pode ser roubada ou emprestada, assim sendo mais seguro utilizá-la do que o sistema convencional de senha.

No Brasil, a emissão de passaporte, de carteiras de identidade e o cadastro das Polícias Civil e Federal contam com sistemas biométricos. (TSE, 2013). Visando o aperfeiçoamento das estratégias que envolvem o processo eleitoral, garantindo que um eleitor tem direito a apenas um voto, a Justiça Eleitoral do Brasil inicializou a implantação do sistema biométrico. Nas eleições municipais de outubro de 2008 foi iniciado o uso da biometria para realizar a identificação dos eleitores em território nacional, trinta unidades foram utilizadas em cada um dos três municípios selecionados. (ABREU, 2012).

1. **MOTIVAÇÃO**

A Segurança da Informação vem sendo considerada desafio do século XXI e destacando-se a cada dia. Milhares de pessoas utilizam a Internet, trocam informações e usam serviços bancários, de comércio eletrônico, serviços públicos federais, estaduais e municipais, de ensino e pesquisa, das redes sociais, dentre outros, constituindo uma ampla rede de atividades digitais. (BRASIL, 2010).

A informação tem sido um elemento indispensável em todas as atividades humanas, especialmente no processo produtivo e no desenvolvimento humano. Na fase inicial do desenvolvimento, os seres humanos não possuíam a consciência de seu valor e nem da necessidade de protegê-la, só ocorrendo com o surgimento do comércio e da consequente competição pelo mercado.

A internet vem proporcionando conectividade em tempo real trazendo consigo um crescimento sem precedentes no volume de informações. E com o seu crescente uso, transações financeiras, transmissão de dados sigilosos, entre outras aplicações que necessitam a validação da identidade dos usuários, tem se tornado cada vez mais frequentes e necessários utilizando mecanismos que auxiliem na segurança e na identificando do usuário. (OTAVIANO, 2007).

Os métodos de autenticação de usuário mais comuns são baseados em senhas, que são sequências de caracteres alfanuméricos que devem ser digitados através de um teclado, largamente difundido em várias aplicações. Infelizmente, este método não é eficaz, uma vez que os usuários definem suas próprias senhas, a tendência é que a escolha seja algo simples, como por exemplo, a sua data de nascimento, nomes dos parceiros, filhos, animais de estimação, número de sua casa, telefone e outras escolhas óbvias, que tendem a enfraquecer a segurança do sistema. Quando uma senha é suficientemente complexa ao ser gerada por um computador, por exemplo, torna-se difícil se ter acesso a algum sistema, porém nem sempre é tão simples recordar a mesma.

A utilização da biometria para autenticação do usuário é uma das maneiras de se resolver os problemas acima citados e garantir a presença do usuário no local onde a operação será feita.

A biometria é usada em numerosos lugares para aperfeiçoar a segurança ou conveniência dos cidadãos. No Brasil, a emissão de alguns documentos contam com sistemas biométricos. Além disso, algumas empresas utilizam 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 e nos bancos para identificar os clientes para ter o acesso as contas facilitando as transações nos caixas eletrônicos. (TSE, 2013).

1. **OBJETIVOS**
   * 1. **Objetivo Geral**

O objetivo desse trabalho é realizar uma pesquisa e desenvolver um protótipo utilizando métodos de reconhecimento de padrões biométricos para internet.

* + 1. **Objetivos Específicos**
* Análise, técnicas e métodos de controle de acesso;
* Descrever os conceitos sobre o reconhecimento biométrico;
* Estudo da estrutura dos métodos de sistemas biométricos;
* Apresentar análise de alguns métodos de autenticação utilizando reconhecimento biométrico;
* Pesquisa na segurança envolvida nas comunicações e armazenamento dos padrões; e
* Desenvolvimento de um protótipo;

1. **ESCOPO**

A proposta desse trabalho é realizar uma pesquisa e desenvolver uma das principais técnicas e métodos para controle de acesso utilizando reconhecimento de padrões biométricos para internet.

Desta forma, o objetivo final deste trabalho é desenvolver uma aplicação que utilizará um padrão biométrico para o controle de acesso. A Figura 2demonstra as fases do trabalho para o processo de reconhecimento do padrão biométrico que será implementado no trabalho.

**Figura 2- Fases para processo de reconhecimento do padrão biométrico**

1. **REVISÃO BIBLIOGRÁFICA**

O objetivo deste capítulo é apresentar os principais conceitos associados à Segurança da Informação como a Biometria, iniciando com sua definição e as principais características. Depois, serão descritos os processos que compõem um sistema biométrico e cada um de seus módulos. Por fim, apresentará as ferramentas utilizadas para o desenvolvimento do trabalho.

1. **Segurança da Informação**

Informação entende-se por um conjunto de dados com valor para determinada empresa ou pessoa, constituindo um recurso de extrema importância na sociedade atual. (ABREU, 2011). Com a utilização de sistemas informatizados integrados por meio de redes de computadores, as informações armazenadas são trafegadas entre estes estão, de uma maneira ou de outra estão inseguranças e sujeitas a várias ameaças que possam prejudicar a integridade destes sistemas.

A segurança da informação nessa situação se mostra indispensável, e até mesmo crítica em alguns casos, para que a integridade das informações dos sistemas não seja atingidas, assim garantindo a redução de riscos de fraudes, erros, roubo e uso indevido das informações.

* + 1. **Princípios básicos da segurança da informação**

Os princípios básicos da segurança da informação são representadas pela a *Figura 3* abaixo:

**Figura 3 - Segurança da Informação: Tríade CIA**

Os conceito de segurança de informação agrupar-se na análise, no planejamento e na implementação da segurança para um determinado conjunto de informações que se deseja proteger, e são definidos a seguir:

* + 1. **Confiabilidade**

A confidencialidade é garantir que a informação é acessível somente por pessoas autorizadas. Manter a confidencialidade implica em assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento. (TCU, 2012).

* + 1. **Integridade**

A integridade mantem a consistência, precisão e confiabilidade de dados ao longo de todo seu ciclo de vida. Consiste na conformidade dos dados armazenados com relação as inserção, alteração e o processamentos autorizados. (TIPTON e KRAUSE, 2009).

* + 1. **Disponibilidade**

Consiste em garantir que as informações estejam acessíveis as pessoas autorizados, a qualquer momento requerido. Manter a disponibilidade de informações implica em garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito. (WHITMAN e MATTORD, 2011).

* + 1. **Mecanismos de segurança**

Um meio de se aplicar e suportar os princípios básicos de segurança da informação é a utilização de mecanismos e controles (físicos e lógicos). (PERREIRA, 2011).

* + 1. **Controles físicos**

O controle físico são medidas de segurança em uma estrutura definida usada para deter ou evitar acesso não autorizado a material delicado. (VACCA, 2012).

* + 1. **Controles lógicos**

Controles lógicos barreiras que impedem ou limitam acesso à informação em meio eletrônico. Exemplos de mecanismos de controles lógicos: criptografia, assinatura digital, senhas e a biometria. (MACHADO, 2012).

* + 1. **Criptografia**

A criptografia é uma ciência de escrever mensagens em forma cifrada ou em código. É um dos principais mecanismos de segurança usados para se proteger as informações. (MARTIN, 2012)

A criptografia maneira de aumentar a segurança de uma mensagem ou arquivo embaralhando o conteúdo de modo que possa ser lido somente por alguém que tenha a chave de criptografia. Por exemplo, comprar algo de um site, as informações para transação (como endereço, número de telefone e número de cartão de crédito) é geralmente criptografado para manter a segurança das informações. (HOFFSTEIN, PIPHER e SILVERMAN, 2014).

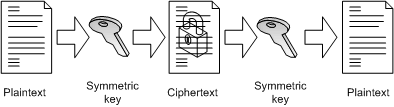
* + 1. **Criptografia Hash**

A criptografia *Hash* permite que *String* seja calculada um identificador digital chamado *Hash*. Esse valor é formado por 16 bytes (no caso do MD-2, MD-4 e MD- 5) ou 20 bytes (no caso do SHA-1). (STALLINGS, 2011).Neste trabalho foi utilizado o MD-5 para a criptografia dos dados que posteriormente ser armazenado no banco de dados. O MD5 um algoritmo que é usado para verificar a integridade dos dados por meio da criação de uma mensagem de 128 bits a partir de dados de entrada (que pode ser uma mensagem de qualquer comprimento).

* + 1. **Chaves Simétricas**

A criptografia simétrica usa a mesma chave para criptografar e para descriptografar os dados. A criptografia simétrica por ser mais simples também é mais rápida que a criptografia assimétrica. É apropriada para criptografia e descriptografar de uma grande quantidade de dados. A Figura ***4*** mostra o processo realizado para fazer a criptografia de uma mensagem.

**Figura 4 - Processo de criptografia simétrica**

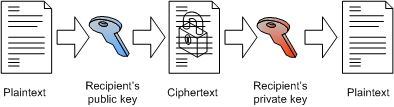


**Fonte:** (TECHNET, 2005)

* + 1. **Chaves Assimétricas**

A criptografia assimétrica utiliza duas chaves diferentes, mas matematicamente relacionadas, para criptografar e descriptografar as informações. As chaves são conhecidas como chaves privadas e chaves públicas. A criptografia assimétrica é mais segura do que a criptografia simétrica, pois a chave usada para criptografar os dados é diferente para descriptografar. Entretanto, como a criptografia assimétrica usa algoritmos mais complexos do que a criptografia simétrica torna o processo mais lento em relação a criptografia simétrica. A mostra o processo de criptografia assimétrica. (TECHNET, 2005)

**Figura 5 - Processo de criptografia assimétrica**



**Fonte:** (TECHNET, 2005)

Criptografia assimétrica somente uma parte mantém a chave privada. Essa parte é conhecida como o assunto. Todas as outras partes podem acessar a chave pública. Os dados criptografados por meio da chave pública só podem ser descriptografados pela chave privada. Por outro lado, os dados criptografados por meio da chave privada só podem ser descriptografados pela chave pública. (STALLINGS, 2011).

* + 1. **Assinatura Digital**

As assinaturas digitais são usadas para vários tipos de documentos assinaturas caneta e tinta, onde tradicionais foram usadas no passado. No entanto, a mera existência de uma assinatura digital não é uma garantia adequada que um documento é o que parece ser. Além disso, as configurações do governo e das empresas muitas vezes precisam impor restrições adicionais em seus fluxos de trabalho de assinatura, como restringir as opções do usuário e o comportamento do documento durante e após a assinatura. Para assinar digitalmente um documento, é necessário ter um ID digital. Esse identificador exclusivo pode ser obtido a partir de várias autoridades de certificação na Web. A assinatura digital é um pequeno bloco de dados que é anexado aos documentos. É gerada a partir do ID digital, o que inclui tanto uma chave privada e pública. A chave privada utiliza para aplicar a assinatura ao documento, enquanto a chave pública é enviada com o arquivo. (PERREIRA, 2011).

* + 1. **Senha**

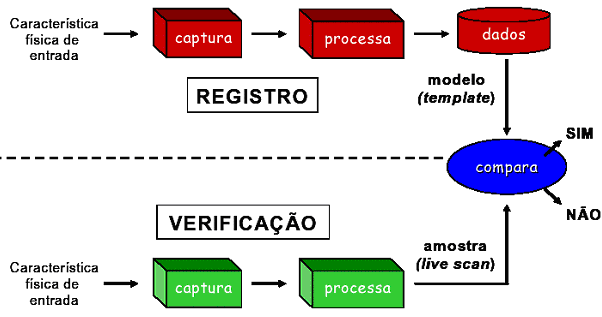
A senha uma palavra ou sequência de caracteres usados para autenticação de usuário. Atualmente nomes de usuário e senhas são usados pelas pessoas durante um log no processo que controla o acesso a sistemas de informação, telefones celulares, caixas eletrônicos, etc. Um usuário comum tem senhas para muitos propósitos: fazer *login* em contas, recuperação e-mail, acessar aplicativos, bancos de dados, redes sociais, web site, etc. Cada método de autenticação tem vantagens e desvantagens em termos de segurança, usabilidade e amplitude de apoio. Métodos de autenticação baseados em senha, no entanto, não fornecem uma forte segurança e não é recomendada a sua utilização. (TCU, 2012).

* + 1. **Biometria**

A Biometria refere-se as métricas relacionadas a características humanas. Autenticação biometria é usada como uma forma de identificação e controle de acesso. Os identificadores biométricos são características distintivas, mensuráveis ​​utilizados para identificar o ser humano classificados como fisiológica e comportamentais. As características fisiológicas estão relacionadas com a forma do corpo, como a impressão digital, palma da mão, reconhecimento do rosto, geometria da mão, o reconhecimento da íris, retina. Características comportamentais estão relacionadas com o padrão de comportamento de uma pessoa, incluindo, digitação e a voz. (BOLLE, CONNELL, *et al.*, 2013).

Os sistemas biométricos utiliza dois mecanismos para autenticação: registro e verificação. O primeiro passo é o reconhecimento da pessoa realizando o cadastro das informações biométricas, sejam ela dados da impressão digital, voz, retina, assinatura, etc. e posteriormente são transformadas em código digital e armazenadas em uma base de dados. Após o armazenando das informações, o segundo passo é realizar o reconhecimento da pessoa através da comparação dos dados armazenadas no instante da solicitação de reconhecimento e dados armazenados no banco de dados.

A Figura 6 representa o processo de registro e verificação em um sistema biométrico.

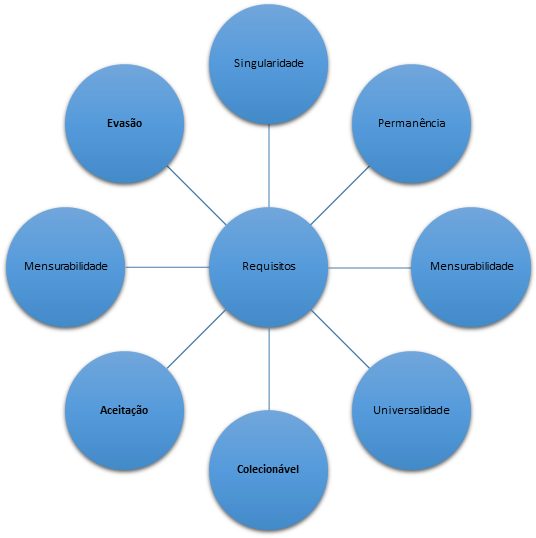
**Figura 6 - Métodos de Biométricos**

**Fonte:** (PINHEIRO, 2008)**.**

Um sistema biométrico faz o reconhecimento do reconhecimento de padrões de características biológicas que realiza operações de aquisição dos dados biométricos, por meio de um hardware especifico para a captura da característica biométrica, a extração das características dos dados adquiridos e a comparação das características com os padrões armazenados na base de dados.

Em um sistema biométrico existem duas abordagem distintas e elas são segundo (ASHBOURN, 2011) :

* **Verificação:** O sistema de verificação executa uma comparação 1:1 da informação de entrada buscando na base de dados as características biométricas sobre o usuário verificando se o usuário diz ser, assim autenticando-o no sistema de informação.
* **Identificação:** O sistema de identificação executa uma comparação 1:N onde o sistema faz a busca em toda a base de dados por algum usuário que tenha se registrado com a mesma informação do sistema que está sendo pesquisado até que seja identificado ou não.



**Figura 7- Requisitos dos Sistemas Biométricos**

A informação utilizada para o reconhecimento de uma pessoa pode ser fisiológica ou comportamental, contudo é importante garantir que alguns critérios no momento da escolha da informação, obedeça os requisitos necessário para o desenvolvimento de um sistema de reconhecimento biométrico, a Figura 7 mostra os requisitos necessário e são definidos logo abaixo segundo (LI, 2009):

* **Universalidade**: Cada pessoa deve ter a característica biométrica e raramente deve perder a um acidente ou doença.
* **Singularidade**: Apenas uma pessoa pode ter o mesmo valor da característica biométrica se ele deve ser distinta entre indivíduos.
* **Permanência**: A característica biométrica não deve mudar a longo do tempo e não deve sofrer alterações consideráveis ​​relativas a idade ou doença.
* **Colecionável**: A característica biométrica deve ser colecionável de qualquer pessoa em qualquer ocasião.
* **Aceitação**: Sociedade e público em geral deve ter nenhuma objeção a fornecer a característica biométrica.
* **Mensurabilidade**: mensurabilidade possibilidade de adquirir e digitalizando a característica biométrica usando alguns dispositivos / sensores digitais adequados, sem causar qualquer inconveniente para a pessoa.
* **Evasão**: A característica biométrica não pode ser imitada ou forjados. A evasão entende-se que o sistema deve ser capaz de lidar com estas situações eficazmente.

Atualmente existem vários tipos de características biométricas que podem ser utilizadas para reconhecimento de uma pessoa. A Figura 8 abaixo apresenta os tipos de biometrias usadas para o reconhecimento.

**Figura 8 - Tipo de características biométricas**

* + 1. **Facial**

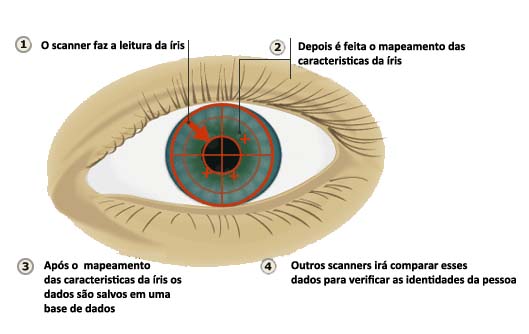
Reconhecimento facial envolve uma avaliação das características faciais verificando automaticamente uma pessoa de uma imagem digital ou um vídeo quadro de uma fonte de vídeo. Uma das técnicas para fazer isto é simplesmente pela avaliação características faciais selecionadas da imagem, bem como a partir do banco de dados facial para fazer a identificação e verificação da característica biométrica. (MARSICO, NAPPI e MASSIMO, 2014).

Sistemas biométricos de reconhecimento facial coleta os dados de rosto dos usuários e armazena em uma base de dados. Será medida a estrutura geral e a proporção de recursos no rosto do usuário, tais como: distância entre olhos, nariz, boca, orelhas, queixo, tamanho dos olhos, boca e outras expressões para fazer a comparação para o reconhecimento da pessoa. (LI e JAIN, 2011).

* + 1. **Iris**

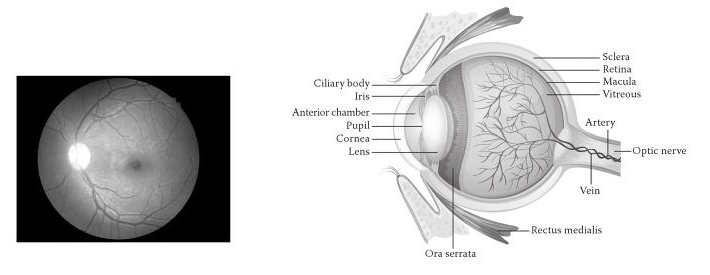
A íris uma região anular do olho delimitada pelo pupila e a esclera (parte branca do olho). A textura visual da íris é formada durante o desenvolvimento fetal e estabiliza durante os dois primeiros anos de vida (a pigmentação, no entanto, continua a mudança ao longo de um período de tempo prolongado. A textura da íris transporta informação útil muito distinta de reconhecimento pessoal. Também controla a quantidade de luz que permitindo proteger a retina do olho. Sistemas de reconhecimento de íris faz a varredura da íris de diferentes maneiras. Faz uma analisar de vários pontos da íris incluindo: anéis, sulcos, sardas, as características corona e outros. Depois fazendo o armazenamento das informações na base de dados. (HOLAMBE e RAHULKAR , 2014). A Figura 9 demostra os passos que são realizado para o reconhecimento da íris.

**Figura 9 - Processo de reconhecimento da Íris**

****

Fonte: Adaptado de (JAIN, 2011)

* + 1. **Retina**

O escaneamento da retina é uma técnica biométrica que utiliza os padrões dos vasos sanguíneos da retina de uma pessoa. A retina humana é um tecido fino composto por células neuronais que estão localizados na parte posterior do olho. Devido à estrutura complexa dos capilares que abastecem a retina com o sangue, a retina de cada pessoa é única. A varredura da retina é realizada através do lançando um feixe de luz infravermelha de baixa energia no olho. Este feixe de luz segue um caminho padronizada sobre a retina. Porque os vasos sanguíneos da retina absorvem a luz mais facilmente do que o tecido circundante, a quantidade de reflexão varia durante a varredura. O padrão de variações é digitalizado e armazenado em uma base de dados. (GUPTA e SING, 2014). A Figura 10 apresenta a vista lateral geral do olho, que inclui tanto a retina e a íris.

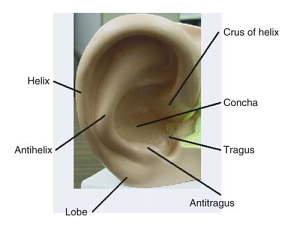
**Figura 10 - Vista lateral da retina**

**Fonte:** (DAS, 2014)**.**

* + 1. **Orelha**

O sistema biométrico de orelha faz o reconhecimento de uma imagem de entrada e em seguida compara com uma base de dados para determinar a sua identidade. O Reconhecimento da orelha pode ser realizado usando um 2D digital imagem da orelha ou uma nuvem de pontos 3D que captura a superfície da orelha. O Reconhecimento da orelha envolve alguns passos. Um dos passos é a localização a posição da orelha na imagem. O sistema utiliza tipicamente um limite retangular para indicar extensão espacial da orelha no lado perfil de imagem de face. O sistema compara as características extraídas a partir da imagem da orelha de entrada com aquelas armazenados na base de dados para estabelecer o a identidade de ouvido. O sistema utiliza as porcentagens para decidir se o usuário diz ser. (BHANU e CHEN, 2010).

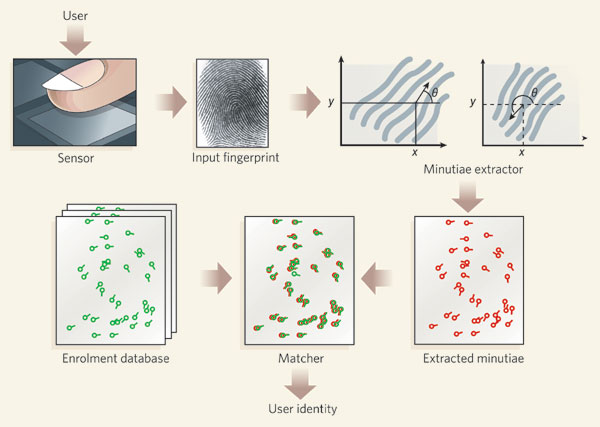
**Figura 11 - Ouvido externo e as partes anatômicas**



Fonte: (SAN e KIM, 2008).

* + 1. **Impressão Digital**

O reconhecimento da impressão digital refere-se ao método automatizado de identificação e confirmação da identidade de um indivíduo, baseado na comparação de duas impressões digitais. A impressão digital é o desenho formado pelas papilas, presentes nos dedos das mãos são únicas em cada indivíduo não pode ser falsificada e nem roupadas, um dos dados biométricos mais conhecidos, e é a solução biométrica mais utilizada para autenticação em sistemas informatizados e a mais estudada na área de segurança desde o século XIX como elemento de identificação A obtenção impressão digital ocorre por meios ópticos, sendo gerada uma imagem para que possa ser feita o processamento pelo sistema, que identificando as características datiloscópicas, comparando com os registros na base de dados, determinando ou não o acesso ao sistema de informação. (SUN, YANG, *et al.*, 2013). A Figura 11 ilustra o processo de reconhecimento e comparação em um sistema de reconhecimento de impressão digital.

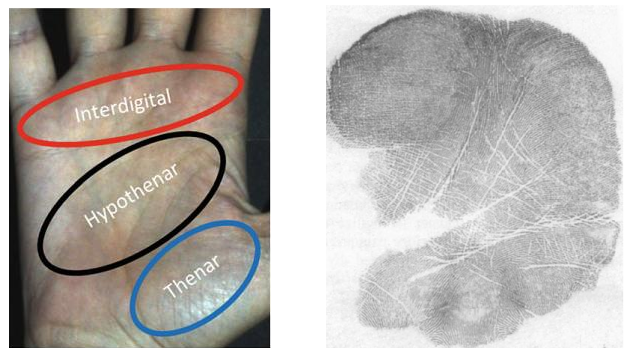


**Figura 12 - Processo de reconhecimento da impressão digital**

**Fonte:** (ANIL , 2007)

* + 1. **Palma da Mão**

Reconhecimento da palma da mão contêm padrão de cordilheiras e vales muito parecido com as impressões digitais. A área da palma da mão é muito maior do que a área de um dedo e, como resultado, espera-se que as impressões palmares é ainda mais distinta do que as impressões digitais. A palma da mão também contém características distintivas, tais como linhas e rugas principais que podem ser capturadas até mesmo com um scanner de resolução mais baixa. Finalmente, ao usar um scanner *palmprint* de alta resolução, todas as características da mão, tais como geometria, cume e vale características (por exemplo, minúcias e pontos singulares, como deltas), linhas principais, e rugas podem ser combinados para construir um de alta precisão sistema biométrico. (JAIN, FLYNN e ROSS, 2008). A Figura 11 apresenta as principais linhas e rugas das mão para realizar o reconhecimento biométrico.



**Figura 13- Principais linhas e rugas da mão**

**Fonte:** (GENOVESE, PIURI e SCOTTI, 2014)**.**

* + 1. **Geometria da Mão**

Os sistemas de reconhecimento da geometria da mão são baseadas em um número de medições efetuadas a partir da mão humana, incluindo a sua forma, tamanho da palma da mão, e os comprimentos e larguras dos dedos. Informações de geometria da mão não são invariável durante o período de crescimento. Além disso, joias de um indivíduo (por exemplo, anéis) ou limitações na habilidade (por exemplo, a partir de artrite), podem representar desafios para extrair as informações geometria da mão correta. O tamanho físico de um sistema baseado em geometria da mão é grande, e não podem ser incorporados em certos dispositivos, como computadores portáteis. Existem sistemas de autenticação disponíveis que são baseados em medições de apenas alguns dedos (tipicamente, indicador e médio) em vez de todo o lado. Estes dispositivos são menores do que as utilizadas para a geometria da mão, mas ainda muito maior do que os utilizados para a aquisição de certas outras características biométricas. (JAIN, FLYNN e ROSS, 2008).

* + 1. **Voz**

A voz uma combinação de características físicas e comportamentais biométricos. As características físicas de voz de um indivíduo são baseados na forma e tamanho dos apêndices (por exemplo, intervalos vocais, boca, das cavidades nasais, e lábios) que são utilizados na síntese do som. Estas características físicas da fala humana são invariantes para um indivíduo, mas o aspecto comportamental das alterações de fala ao longo do tempo devido à idade, condições médicas (como o resfriado comum), estado emocional, etc. Uma desvantagem de reconhecimento de voz é baseada em características de fala que são sensíveis a um número de fatores tais como ruído. Reconhecimento de voz é mais apropriado em aplicações baseadas no telefone, mas o sinal de voz é normalmente degradado em qualidade pelo canal de comunicação. (JAIN, FLYNN e ROSS, 2008).

* + 1. **Assinatura**

A assinatura forma de como uma pessoa assina seu nome e é conhecida por ser uma característica que cada pessoa tem. Embora as assinaturas exigem contato com o instrumento de escrita e um esforço por parte do usuário, eles foram aceitos em transações do governo, legais e comerciais como um método de autenticação. A assinatura é uma característica biométrica comportamental que muda ao longo de um período de tempo e influenciada pelas condições físicas e emocionais de algumas pessoas variam consideravelmente, até mesmo impressões sucessivas de sua assinatura são significativamente diferentes Além disso, os falsários profissionais pode ser capaz de reproduzir assinaturas que enganar o sistema de verificação de assinaturas. (SAN e KIM, 2008).



**Figura 14- Sistema de verificação de assinatura on-line**

**Fonte:** (REVETT, 2008)**.**

* 1. **FERRAMENTAS UTILIZADAS PARA O DESENVOLVIMENTO**

Essa seção apresenta as ferramentas utilizadas para o desenvolvimento do trabalho.

* + 1. **Python**

Python uma linguagem de programação orientada a objetos interpretada de alto nível com semântica dinâmica. Construída por estruturas de dados, combinado com tipagem dinâmica e ligação dinâmica, torná-lo o desenvolvimento da aplicação muita rápida. Tem uma sintaxe simples, enfatiza a legibilidade e, portanto, reduz o custo de manutenção do programa. Python suporta módulos e pacotes, o que incentiva a modularidade programa e reutilização de código. O interpretador Python e sua extensa biblioteca padrão estão disponíveis em fonte ou forma binária sem encargos para todas as principais plataformas, e pode ser distribuído livremente. (SUMMERFIELD, 2013).

* + 1. **We2bpy**

Web2py um *framework full-stack* o*pen source* para desenvolvimento rápido da aplicação. O *framework* não requer instalação e não tem arquivos de configuração, inclui um servidor web, banco de dados e um IDE baseado na web. O web2py possui o *Database Abstraction Layer* (DAL) que elimina *SQL Injections*. O modelo de linguagem impede a vulnerabilidade de *Cross Site Request Forgeries.* (PIERRO, 2012)*.*

* + 1. **OpenCV**

Uma biblioteca de código aberto, que possui vários algoritmos de visão computacional. Esses algoritmos são usados ​​para detectar e reconhecer rostos, identificar objetos, classificar as ações humanas em vídeos, movimentos de câmera pista, objetos de pista em movimento, extrair modelos 3D de objetos, produzir nuvens de pontos 3D a partir de câmeras estéreo, ponto em conjunto para produzir imagens de alta resolução imagem de uma cena inteira, encontrar imagens similares de um banco de imagens, remover olhos vermelhos de imagens tiradas com flash, reconhecer cenário e estabelecer marcadores para cobri-la com a realidade aumentada, etc. (OPENCV, 2014).

* + 1. **PostgresSQL**

Os dados biométricos após o processamento da imagem e da extração das característica está sendo utilizado o PostgreSQL para o armazenamento dos dados criptografados. É um sistema de gerenciamento de banco de dados objeto-relacional (ORDBMS), a principal função é armazenar dados de forma segura, apoiando as melhores práticas, e para permitir a recuperação, a pedido de outras aplicações de software. O SGBD permite lidar com cargas de trabalho que vão de pequenas aplicações a aplicações de grandes porte para a Internet, com muitos usuários simultâneos. (SMITH, 2010).

1. **DESENVOLVIMENTO**
2. **Elementos Biométricos**

Entre os principais tipos de elementos biométricos pode ser identificados sistemas baseados na identificação física (impressão digital, reconhecimento facial, geometria da mão, reconhecimento íris e retina, entre outros) ou comportamental (reconhecimento da voz, digitação, assinatura, etc.). Os critérios para a escolha de uma característica biométrica são consideradas o conforto na utilização, a precisão, a relação entre a qualidade e o preço e o nível de segurança.

A Tabela 1 apresenta uma comparação realizada por (HOLAMBE e RAHULKAR , 2014) entre as principais características biométricas mais utilizadas no reconhecimento de uma pessoa. Nenhuma das características biométricas comparadas possui um grau elevado em todos os requisitos comparados, assim fazendo com que nenhuma seja considerada excelente. No entanto, a característica biométrica que apresenta um bom equilíbrio é a impressão dentre todas as características comparadas.

**Tabela 1 - Comparação das características biométricas mais utilizadas**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Característica** | **Universalidade** | **Unicidade** | **Permanência** | **Coletabilidade** | **Desemprenho** | **Aceitabilidade** | **Coletabilidade** |
| **Geometria da Mão** | Média | Média | Média | Média | Méda | Média | Baixa |
| **Orelha** | Média | Média | Alta | Média | Média | Alta | Média |
| **Impressão Digital** | Média | Alta | Alta | Média | Alta | Média | Média |
| **Face** | Alta | Baixa | Média | Alta | Baixa | Alta | Alta |
| **Retina** | Alta | Alta | Média | Baixa | Alta | Baixa | Baixa |
| **Iris** | Alta | Alta | Alta | Média | Alta | Baixa | Baixa |
| **Voz** | Média | Baixa | Baixa | Média | Baixa | Alta | Alta |
| **Assinatura** | Baixa | Baixa | Baixa | Alta | Baixa | Alta | Alta |

**Fonte**: Adaptada de (HOLAMBE e RAHULKAR , 2014)

* 1. **Modelo escolhido – Impressão Digital**

Dentre as características biométricas apresentada neste trabalho, a impressão digital é a mais estudada, sendo utilizada na área de segurança desde o século XIX como elemento de identificação pessoal. As impressões digitais são únicas para cada ser humano e também considerado o tipo biométrico mais seguro para determinar a identidade depois do teste de DNA. (PINHEIRO, 2008).

* 1. **Aquisição da Imagem**

O processo de aquisição é o processo de obtenção dos dados da característica biométrica oferecida. Neste trabalho está sendo utilizado o sensor biométricos FS80 representado pela a Figura 15 que utiliza a tecnologia de sensor CCD para entregar a imagem da impressão digital de alta qualidade.O dedo é iluminado por 4 LEDs infravermelhos durante a digitalização e a intensidade da luz é ajustada automaticamente de acordo com a digitalização de impressões digitais características (molhada, seca, turva, etc) para otimizar a qualidade da imagem digital capturada.

****

Figura 15 - Leitor Biométrico

* 1. **Processamento de impressões digitais**

O processo de aquisição da impressão digital através de uma sensor, porém no processo de captura da imagem podem sofrer imperfeições, ou ainda, não estarem em condições ideais para servir como entrada a um classificador, por esse motivo, existe a necessidade de uma fase de processamento nas imagens, conhecida como pré-processamento, que consiga remover os ruídos encontrados nas imagens, ou seja, eliminar erros provocados na fase anterior (aquisição), e preparar a imagem para as fases seguintes (extração de características e identificação) conforme a Figura 16. Essa preparação tem como objetivo facilitar e agilizar a execução da fase de classificação.



Figura 16- Imagem Capturada pelo Sensor

O SIFT a introduzido por (LOWE, 1999) permite que a extração das característica de uma imagem, invariante de escala, rotação e transformações de tradução e também invariável a alterações na iluminação. Depois de uma vistosa refinamento das características SIFT, um conjunto reduzido de ponto-chaves é obtido. Estes postos-chaves estão localizadas nas regiões singulares (Caracterizada por uma elevada curvatura cume) e sobre as regiões alterados (caracterizado por cristas fragmentados, um grande número de terminações cume e incomum bifurcações).

* + 1. **SIFT(Scale Invariant Feature Transform)**

*Scale Invariant Features Transform* (SIFT) publicado por David Lowe em 1999 é um algoritmo de visão computacional para detectar e descrever os recursos locais em imagens. Usado por possuir propriedade de ser fortemente invariante às mudanças de rotação, escala, ponto de vista e iluminação. (LOWE, 1999).

Desenvolvido para resolver o problema de equivalência entre imagens incluindo o reconhecimento de objetos, mapeamento e navegação robótica, imagem costura, modelagem 3D, reconhecimento de gestos, rastreamento de vídeo, identificação individual de animais selvagens e jogo em movimento.

O algoritmo SIFT é executado através de cinco etapas principais segundo (LOWE, 1999):

* **Scale-space Extrema Detection**

Primeira fase do SIFT consiste em detectar os pontos de interesse invariante a mudanças de escala da imagem, que são chamados key-points no SIFT. Para isto, a imagem passa pelo filtro de Gauss em diferentes escalas. Pontos-chave são então tomados como valores máximos / mínimos da diferença de gaussianas que ocorrem em múltiplas escalas.

A imagem é determinada por L(x,y,σ), esta função produz uma convolução de uma função de Gauss, G(x,y,σ), com a imagem, I(x,y) conforme a Equação abaixo:

(1)

Este filtro varia à escala pelo o parâmetro σ, na Equação 2:

(2)

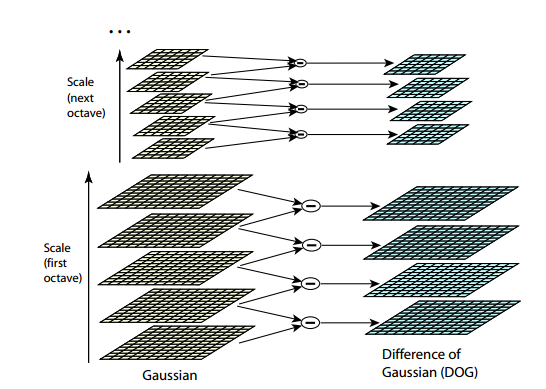
A busca dos pontos-chave utiliza a função Difference of Gaussian (DoG) composta pela diferença de imagens filtradas em escalas próximas, apenas separadas por uma constante de escala k. A função DoG é definida pela Equação 3:

(3)

O resultado da convolução da imagem com o filtro DoG é dada pela equação 4:

(4)

A função DoG suaviza as imagens sendo calculada pela subtração das imagens desfocadas pelo filtro Gaussiano em escalas σ e kσ. Esta função obtém amostra da imagem eliminando detalhes e ruídos indesejados e as características são realçadas. A Figura 15 apresenta a função DoG.



**Figura 17- Representação da obtenção das DoG para as oitavas de uma imagem**

Fonte: (LOWE, 1999).

* **Keypoint Localization**

Para a detecção dos locais máximos e mínimos de D (x, y, σ), cada ponto de amostra é comparado com os seus oito vizinhos na imagem atual e nove vizinhos na escala acima e abaixo conforme aFigura 18**.** Ele é selecionado somente se ele é maior do que todos esses vizinhos ou menor do que todos deles. O custo dessa verificação é razoavelmente baixo devido ao fato de que a maioria dos pontos de amostragem será ser eliminado seguindo as primeiras verificações.

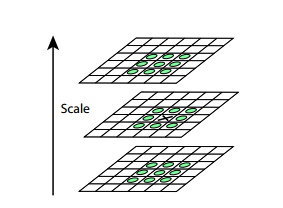
****

Figura 18 - Máximos e mínimos das imagens diferença-de-Gaussian são detectados por comparação de um pixel (marcado com X) para seus 26 vizinhos em regiões de 3x3 nas escalas atuais e adjacentes (marcados com círculos).

**Fonte:** (LOWE, 1999)**.**

* **Orientation Assignment**

A escala do ponto chave é usada para selecionar a imagem suavizada pela Gaussiana L, com a escala mais próxima, de modo que toda a computação seja realizada de modo invariante à escala. O gradiente de magnitude m(x,y) é calculado com a Equação 4.

Em seguida, é construído um histograma de orientação (36 bins) a partir das orientações dos gradientes dos pontos amostrados, com uma região ao redor do ponto chave e, os picos neste histograma correspondem à direção dominante do gradiente local. Orientações com frequência acima de 80% do valor do pico no histograma são usadas para criar pontos chave com essa orientação. Desta forma, para múltiplas orientações de magnitude similar, existem múltiplos pontos chave criados no mesmo local e escala, mas com diferentes orientações.

* **Keypoint Descriptor**

Após a localização, escala e orientação da imagem ter sido atribuída a cada ponto chave, é possível adotar um sistema de coordenadas bidimensional para descrever a região local da imagem e prover invariância com respeito a esses parâmetros. O próximo passo é calcular um descritor para a região da imagem local que é distinta e invariante a variações adicionais, tais como mudanças na iluminação ou ponto de vista 3D. Para alcançar a invariância de orientação, as coordenadas do descritor e as orientações do gradiente são rotacionadas em relação à orientação do ponto chave. Este procedimento é mostrado na Figura 1, onde o descritor de um ponto chave é criado pela determinação da magnitude e orientação do gradiente em cada pixel da imagem amostrada em uma região ao redor do ponto chave, como mostrado em (a). Os descritores são ponderados em uma janela Gaussiana indicada pelo círculo. Estas amostras são acumuladas em histogramas de orientação, como exibido em (b)

* **Keypoint Matching**
  + 1. **cvtColor e threshold**

A função cvtColor converte uma imagem de entrada a partir de um espaço de cor para outro. Assim, o primeiro byte de uma imagem de cor normal (24 bits) irá ser um componente azul de 8 bits, o segundo byte será verde, e o terceiro byte será vermelho. Os quarto, quinto, sexto e bytes, então, seria o segundo pixel (Azul, Verde, em seguida, em seguida, o vermelho), e assim por diante.

A função threshold usado para obter uma imagem de nível binário uma imagem em tons de cinzento ou para a remoção de um ruído, isto é, filtrando os pixels com muito pequena ou muito grande valores. A Figura 19 apresenta a função de melhoramento da imagem para a aquisição da características biométrica. O resultado da execução da função é apresentada na Figura 20.

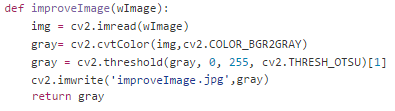
****

Figura 19 - Melhoramento da Imagem

****

Figura 20 - Antes e Depois do uso das funções cvtColor e threshold

* + 1. **skeletonization**

Skeletonization é uma versão fina de forma que que é equidistante até aos seus limites. O esqueleto geralmente enfatiza propriedades geométricas e topológicas de forma, como a sua conectividade, topologia, comprimento, direção e largura. Juntamente com a distância dos seus pontos de forma a fronteira, o esqueleto pode também servir como uma representação da forma (que contém todas as informações necessárias para reconstruir a forma).



Figura 21- Skeletonization da Impressão digital

* 1. **Extração de caraterísticas**
     1. **Keypoints**

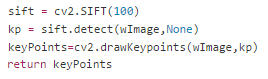
Para fazer a extração das características biométricas de uma pessoa foi utilizado também o SIFT que devolve características que são chamados de keypoints encontrados na imagem. Os keypoints são coordenadas (x,y) na imagem como pode ser visto na Figura 22. Para a detecção dos keypoints é necessário criar um objeto SIFT com a quantidade de keypoints para a detecção das características biométricas de uma pessoa.

.

****

Figura 22 - Keypoints

A Figura 23 apresenta um trecho da detecção das características biométricas de uma pessoa. A função cv2.detect() localiza os keypoitns na imagem, cada keypoint é uma estrutura que tem as coordenadas (x,y), tamanho, vizinhança e ângulo. A Função cv2.drawKeypoints() responsável em desenha os keypoints na imagem conforme a figura 22.

****

.

Figura 23 - Código de detectar os keypoints

* 1. **Armazenamento e segurança**

Para a criptografia dos pontos chaves do usuário foi utilizado a criptografia hash MD5.O MD5 é um algoritmo que é usado para verificar a integridade dos dados por meio da criação de uma mensagem de 128 bits (16 bytes) a partir de dados de entrada geralmente expressa no formato hexadecimal de 32 dígitos. A Figura 24 apresenta a função desenvolvida para fazer a criptografia dos keypoints do usuário.



Figura 24 - Criptografia dos Keypoints

A Figura 25 apresenta a função completa para criptografia dos keupoints do usuário. A função percorre todos os keypoints e detecta todos os pontos. O detector gera vários níveis de recursos. As características de cada nível estão localizadas nos nós de uma grade regular sobre a imagem conforme a

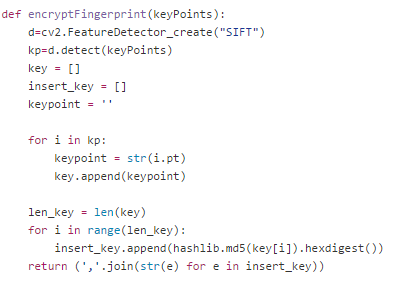
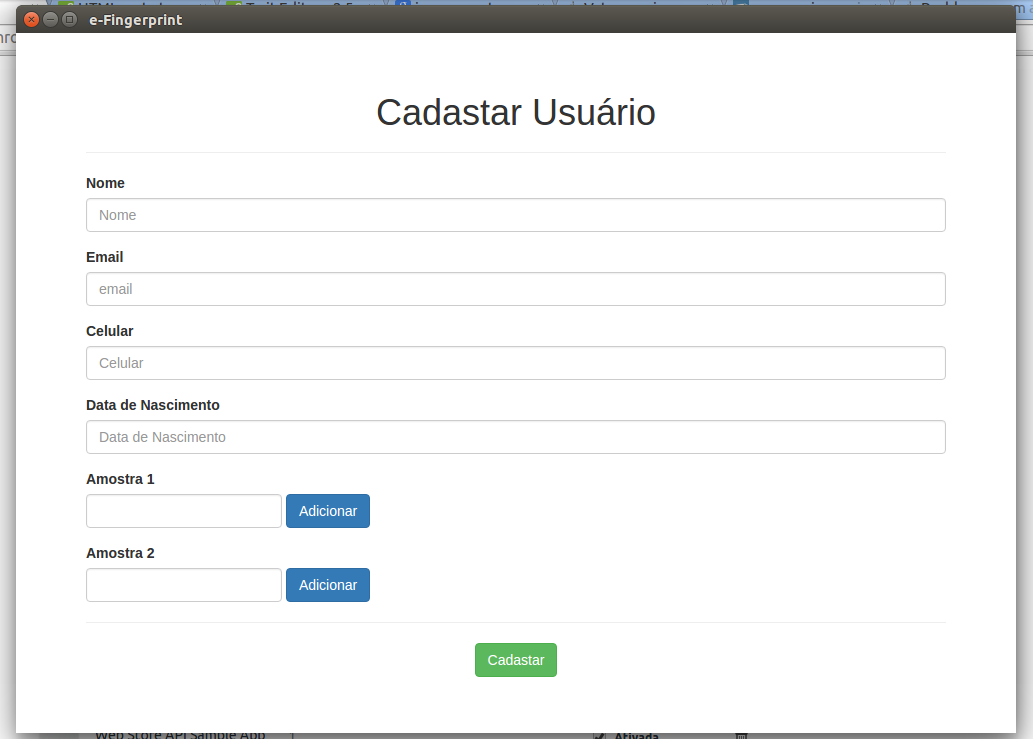
****

Figura 25 - Função completa de criptografia dos Keypoints



* 1. **Comparação**

Para se encontrar a correspondência (matching) entre duas imagens, é possível usar os pontos chave detectados com o algoritmo SIFT. Cada ponto chave está associado a um vetor de descritores com 128 dimensões, a comparação desses descritores torna possível encontrar a correspondência de uma imagem com outra. Lowe [17] provou que a melhor correspondência para cada ponto chave é encontrada pela identificação de seus vizinhos mais próximos, que é definida minimizando a distância Euclidiana para os vetores de descritores. Para evitar uma busca exaustiva, Lowe [17] sugere o uso de uma estrutura de dados k-d tree [4], que suporta uma busca binária balanceada para encontrar o vizinho mais próximo dos descritores. O algoritmo heurístico Best-Bin-First (BBF) é usado nesta busca, pois retorna o vizinho mais próximo, com alta probabilidade.

1. **RESULTADO**
2. **CONSIDERAÇÕES FINAIS**
3. **REFERÊNCIAS**

ABREU, G. M. D. Recadastramento Biométrico. **Resenha Eleitoral**, 2012. Disponivel em: <http://www.tre-sc.jus.br/site/resenha-eleitoral/edicoes-impressas/integra/arquivo/2012/junho/artigos/a-introducao-das-eleicoes-biometricas-no-brasil/index1738.html?no\_cache=1&cHash=ec7a5ef6338feab45f8410a7d419fb9f>. Acesso em: 26 dez. 2014.

ABREU, L. F. D. S. **A Segurança da Informação nas Redes Sociais**. São Paulo. 2011.

ANIL , J. K. Technology: Biometric recognition. **Nature**, Setembro 2007.

ASHBOURN, J. **Guide to Biometrics for Large-Scale Systems:** Technological, Operational, and User-Related Factors. [S.l.]: Springer, 2011.

BARROS, O. S. R.; GOMES, U. D. M.; FREITA, W. L. D. **Desafios estratégicos para segurança e defesa cibernética**. Brasília: [s.n.], 2011.

BHANU , B.; CHEN,. **Human Ear Recognition by Computer**. [S.l.]: Springer, 2010.

BOLLE, M. et al. **Guide to Biometrics**. [S.l.]: Springer, 2013.

BRASIL, C. G. D. I. N. **Cartilha de Seguranc¸a para a Internet**. São Paulo: CERT, 2012.

BRASIL, P. D. R. G. D. S. I. D. D. **Livro verde:** segurança cibernética no Brasil. Brasília: [s.n.], 2010.

DAS, R. **Biometric Technology:** Authentication, Biocryptography, and Cloud-Based Architecture. [S.l.]: CRC Press , 2014.

GENOVESE, A.; PIURI, ; SCOTTI,. **Touchless Palmprint Recognition Systems**. [S.l.]: Springer, 2014.

GUPTA , ; SING,. **Advances in Biometrics for Secure Human Authentication and Recognition**. [S.l.]: CRC Press, 2014.

HOFFSTEIN, ; PIPHER, ; SILVERMAN, H. **An Introduction to Mathematical Cryptography**. 2ª. ed. [S.l.]: Springer, 2014.

HOLAMBE, R. S.; RAHULKAR ,. **Iris Image Recognition:** Wavelet Filter-Banks Based Iris Feature Extraction Schemes. New York: Springer, 2014.

JAIN, A. K.; FLYNN, P.; ROSS, A. A. **Handbook of Biometrics**. [S.l.]: Springer, 2008.

JAIN, R. A Survey of Biometrics Security Systems, 2011. Disponivel em: <http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/>. Acesso em: 30 maio 2015.

LI , S. Z.; JAIN, A. K. **Handbook of Face Recognition**. London: Springer, 2011.

LI, S. Z. **Encyclopedia of Biometrics Recognition**. [S.l.]: Springer, 2009.

LOWE, D. G. Object recognition from local scale-invariant features. **The Proceedings of the Seventh IEEE International Conference on Computer Vision**, Vancouver, v. 2, jul. 1999.

MARSICO, M. D.; NAPPI, ; MASSIMO, T. **Face Recognition in Adverse Conditions**. [S.l.]: IGI Global , 2014.

MARTIN, K. M. **Everyday Cryptography:** Fundamental Principles and Applications. [S.l.]: OUP Oxford , 2012.

NSTC, N. S. A. T. C. **biometrics**, 2006. Disponivel em: <http://www.biometrics.gov/documents/biofoundationdocs.pdf>. Acesso em: 05 maio 2015.

OPENCV, 2014. Disponivel em: <http://docs.opencv.org/2.4.9/modules/refman.html>. Acesso em: 16 maio 2015.

OTAVIANO, C. H. Biometria: Seus métodos e aplicações, Dourados, 2007. Disponivel em: <http://www.uems.br/portal/biblioteca/repositorio/2011-08-11\_20-32-15.pdf>. Acesso em: 23 dez. 2014.

PEREIRA, D. D. S. A. et al. Métodos de processamento e tratamento de imagens para reconhecimento facial. **XI Encontro Latino Americano de Iniciação Científica e VII Encontro Latino Americano de Pós-Graduação – Universidade do Vale do Paraíba**, p. 35-38, 2007.

PERREIRA, M. N. **Processo Digital - A Tecnologia aplicada como garantia da celeridade processual**. 1ª. ed. São Paulo: Biblioteca24horas, 2011.

PIERRO, M. D. **Web2py**. [S.l.]: [s.n.], 2012.

PINHEIRO, F. P. **A CIBERNÉTICA COMO ARMA DE COMBATE**. Rio de Janeiro: [s.n.], 2013.

PINHEIRO, J. M. D. S. **Biometria nos Sistemas Computacionais:** Você é a Senha. [S.l.]: Editora Ciência Moderna, 2008.

RATHA, N. K.; GOVINDARAJU, V. **Advances in biometrics:** sensors, algorithms and systems. New York, USA: pringer-Verlag London, 2008.

REVETT, K. **Behavioral Biometrics:** A Remote Access Approach. [S.l.]: John Wiley & Sons, 2008.

SAN , ; KIM, S.-W. **Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications**. [S.l.]: Springer, 2008.

SMITH, G. **PostgreSQL 9.0 High Performance**. [S.l.]: Packt Publishing, 2010.

STALLINGS, W. **Cryptography and Network Security Principles and Practice**. 5ª. ed. [S.l.]: Pearson, 2011.

SUMMERFIELD, M. **Python in Practice:** Create Better Programs Using Concurrency, Libraries, and Patterns. [S.l.]: Addison-Wesley, 2013.

SUN, Z. et al. **Biometric Recognition**. 8ª. ed. [S.l.]: Springer, 2013.

TCU, T. D. C. D. U.-. **Boas Práticas em Segurança da Informação**. 4 ª. ed. Brasília: [s.n.], 2012.

TECHNET. Usando criptografia de SQL Server 2005 para ajudar a proteger dados. **TechNet**, 2005. Disponivel em: <https://technet.microsoft.com/pt-br/library/bb735261.aspx>. Acesso em: 03 maio 2015.

TIPTON, F.; KRAUSE,. **Information Security Management Handbook**. 6ª. ed. [S.l.]: CRC Press, 2009.

TSE. **Tribunal Superior Eleitoral**, 2013. Disponivel em: <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/biometria-1>. Acesso em: 04 abr. 2015.

VACCA, J. R. **Computer and Information Security Handbook**. 2ª. ed. [S.l.]: Newnes, 2012.

WAXMAN, O. B. These Are The 25 Worst Passwords of 2014. **Time**, 20 Janeiro 2015. Disponivel em: <http://time.com/3672431/worst-passwords/>. Acesso em: 04 Maio 2015.

WHITMAN, ; MATTORD,. **Principles of Information Security**. 4ª. ed. [S.l.]: Paperback, 2011.

[**http://iris.sel.eesc.usp.br/wvc/Anais\_WVC2012/pdf/97147.pdf**](http://iris.sel.eesc.usp.br/wvc/Anais_WVC2012/pdf/97147.pdf)

O SIFT (Scale-Invariant Feature Transform) [10], é um algoritmo para obtenção de pontos de interesse em imagens. O seu funcionamento é dividido em fases, onde as imagens são analisadas e adaptadas individualmente. O algoritmo começa por identificar os locais candidatos a pontos-chave, como máximos e mínimos locais no histograma de uma região da imagem. Depois é feita uma interpolação dos pontos com baixo e alto contraste. Em objetos com bordas circulares, como no caso das moedas, primeiro é localizada melhor circunferência na borda, nessa circunferência o ponto de interesse será o centro. Os outros pontos são rejeitados para melhorar a precisão. Os pontos que sobrevivem à filtragem são atribuídos uma orientação, baseada nas direções dominantes dos gradientes espaciais. Após a atribuição de orientação, cada ponto chave poderá ser calculado em relação a outro ponto, escala e orientação. Finalmente o cálculo dos descritores é feito para cada ponto dividindo o espaço entorno do ponto chave em uma grade, depois é calculado o histograma de cada quadrado da grade, concatenando os histogramas em um vetor. Cada elemento desse vetor é considerado um ponto de interesse [10]. Na Figura 4, é demonstrado uma aplicação do algoritmo SIFT [10] para identificar os pontos de interesse em duas imagens de uma placa, e depois compara com os pontos de interesse identificados nas imagens.

**http://www.repositoriobib.ufc.br/000012/0000127e.pdf**