Fundação Educacional do Município de Assis
Instituto Municípal de Ensino Superior de Assis - IMESA

TIAGO BARQUILHA SERRANO

PADRÕES BIOMÉTRICOS PARA IDENTIFICAÇÃO

Assis
2010

TIAGO BARQUILHA SERRANO

PADRÕES BIOMÉTRICOS PARA IDENTIFICAÇÃO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação.

Orientadora: Prof.ª Dr.ª Marisa Atsuko Nitto

Área de Concentração: Informática

Assis
2010

FICHA CATALOGRÁFICA

SERRANO, Tiago Barquilha.
Padrões Biométricos Para Identificação / Tiago Barquilha Serrano. Fundação Educacional do Município de Assis – FEMA – Assis, 2010.
130p.

Orientadora: Prof.ª Dr.ª Marisa Atsuko Nitto.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Biometria. 2. Impressão Digital. 3. Reconhecimento.

CDD: 001.6
Biblioteca da FEMA

PADRÕES BIOMÉTRICOS PARA IDENTIFICAÇÃO

TIAGO BARQUILHA SERRANO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Bacharelado em Ciência da Computação, analisado pela seguinte comissão examinadora:

Orientadora: Prof.ª Dr.ª Marisa Atsuko Nitto

Analisador: Prof. Dr. Almir Rogério Camolesi

Assis
2010

DEDICATÓRIA

Dedico este trabalho ao meu pai, ***Odemir Barquilha Serrano****, minha mãe,* ***Solange Carvalho Serrano****, minha irmã,* ***Flávia Barquilha Serrano*** *por sempre me apoiarem, incentivarem e valorizarem meus esforços. Indubitavelmente, a razão mais forte da minha existência. A minha namorada,* ***Andréia de Souza Silva****, pela compreensão durante minhas ausências, pelo seu companheirismo, sua ajuda e incentivo.*

AGRADECIMENTOS

A **Deus**, por tudo, muito obrigado!

A minha orientadora **Prof.ª Dr.ª Marisa Atsuko Nitto**, pela orientação segura durante a realização deste trabalho. Muito obrigado por todo apoio, paciência, disponibilidade, esforço e conhecimento prestados à minha carreira profissional.

A **Fundação Educacional do Município de Assis – FEMA**, por tornar-me capacitado para desenvolver este trabalho.

Aos **professores** do Curso de Ciência da Computação da FEMA, pelos valiosos ensinamentos durante a minha passagem pela instituição.

Aos funcionários e estagiários do **Centro de Pesquisa em Informática – CEPEIN**, por toda a experiência por mim adquirida durante meu estágio.

Aos **amigos** de curso, pelo apoio, amizade e demonstração de companheirismo.

A **todos** que direta ou indiretamente, contribuíram para a realização deste trabalho.

RESUMO

A forma encontrada para registrar pessoas em quase todo o mundo sempre foi à impressão digital e fotos, que são registradas em fichas e permitem a identificação sem maiores problemas. Entretanto, o número de produtos e serviços que envolvem a identificação de indivíduos tem crescido fortemente nos últimos anos. Com isso, por utilizar características biológicas ou comportamentais no processo de identificação, a biometria tem vindo a ganhar relevância, pois é mais simples e conveniente que a memorização de senhas e não exige que o usuário possua algum objeto para ser identificado.

Neste projeto foi desenvolvido um sistema biométrico que utiliza dois procedimentos de reconhecimento. O primeiro é quando o usuário se apresenta como sendo uma determinada pessoa e o sistema compara a veracidade da informação. Sistemas desse tipo são chamados de 1-1 (um-para-um), pois a medida biométrica apresentada é simplesmente comparada com o que foi registrado no banco de dados durante o cadastramento desse usuário. O segundo é quando a identificação de um usuário ocorre a partir do dado biométrico dele e, então, se faz uma busca no banco de dados, comparando as informações até que seja encontrado ou não um registro equivalente ao que está sendo procurado. Estes sistemas são conhecidos por 1-n (um-para-muitos), porque o dado de uma pessoa é comparado ao registro de várias outras.

Para o desenvolvimento do sistema biométrico foi utilizada a linguagem Java, tendo em vista que ela é adequada para garantir a expansão dessas tecnologias. A tecnologia baseada em biometria possui vários recursos associados, como banco de dados e aplicativos, o que facilita muito os desenvolvedores em seus projetos.

.

Palavras Chaves: Biometria; Impressão Digital; Reconhecimento.

ABSTRACT

The way to register people found almost everywhere in the world has always been by fingerprint and photos, which are recorded on cards and allow identification without major problems. However, the number of products and services that involve the identification of individuals has grown strongly in the recent years. Thus, by using biological or behavioral characteristics in the process of identification, biometrics is growing because it is simpler and more convenient than recording passwords and doesn’t require that the user has an object to be identified.

In this project we developed a biometric system that uses two recognition procedures. The first is when the user presents himself as a determined person and the system compares the accuracy of the information. Such systems are called 1-1 (one-to-one), because the biometric measurement is presented simply compared to what was recorded in the database during the registration of that user. The second is when the identity of a user occurs from the biometric data, and then it becomes a search in the database, comparing the information until an equivalent record is found or not compared to one that has being sought. These schemes are known by 1-n (one-to-many), because as a person's record is compared to several others.

For the development of biometric systems was used the Java language, considering that it is appropriate to ensure the expansion of these technologies. The technology based on biometrics has several related resources, such as databases and applications, which greatly facilitate developers in their projects.

Keywords: Biometrics; Fingerprint; Recognition.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 - INTRODUÇÃO

Neste capítulo será feita uma descrição do contexto em que o projeto está inserido, assim como os objetivos e as justificativas para o desenvolvimento do tema escolhido.

1.1 – CONTEXTO

A quantidade de informações no mundo digital tem aumentado por conta da variedade de aplicações em nossa sociedade eletronicamente conectada. Isso faz com que meios mais seguros para sua proteção sejam adotados. A identificação pessoal dos usuários está associada à possibilidade de acesso a essas informações, sendo um dos principais aspectos a serem considerados para garantir a segurança.

Em um sistema computacional, o conceito de segurança está relacionado à verificação de três propriedades: a confidencialidade, que garante o sigilo da informação e que está somente seja divulgada com permissão; a integridade, que é a garantia de que a informação não seja alterada sem uma autorização apropriada; e a disponibilidade, garantindo que a informação seja acessível somente aos devidos usuários (COSTA; OBELHEIRO; FRAGA, 2006).

Os mecanismos de identificação tradicionais baseados em algo que se conhece ou possui já não satisfazem os requisitos de segurança, uma vez que estão propensos a fraudes: podem ser facilmente esquecidos, perdidos, roubados ou copiados, além de não garantir o vínculo entre uma operação e o indivíduo que a realiza. Isso fez com que a demanda por produtos de segurança baseados em sistemas biométricos aumentasse consideravelmente. Na biometria, a identificação é obtida, com um elevado grau de confiabilidade, a partir de características biológicas ou comportamentais que são únicas em cada indivíduo (PRABHAKAR, 2001).

A tecnologia biométrica, baseada em características pessoais, já vem sendo utilizada há alguns anos pela comunidade de segurança computacional. Entretanto, até pouco tempo sua adoção se restringia a ambientes de alta segurança em grandes organizações e aplicações de identificação criminal. Com o aperfeiçoamento da tecnologia o custo dos dispositivos vem caindo e a biometria se popularizando, sendo frequentemente apontada como uma solução promissora para problemas de identificação pessoal (COSTA, 2007).

Os sistemas biométricos funcionam essencialmente da mesma forma: são compostos basicamente pelo registro das características biométricas e pelo reconhecimento das mesmas como um sistema de reconhecimento de padrões. Existem numerosas características físicas e comportamentais do ser humano que podem ser usadas como identificadores biométricos, porém, a impressão digital é a tecnologia biométrica mais utilizada por apresentar o melhor custo benefício entre todas as demais técnicas biométricas (FARIA, 2005).

A impressão digital de um indivíduo consiste na representação gráfica das riscas presentes na ponta de cada um dos seus dedos. Ela é uma característica biométrica que permite fazer o reconhecimento de um indivíduo e há anos tem sido utilizada com este propósito em diversas áreas. O que a princípio era feito de forma manual, com o avanço da tecnologia, tem-se tornado um processo automático que visa facilitar a vida das pessoas que necessitam de tal recurso em seu cotidiano nas mais variadas situações.

Neste projeto foi desenvolvido um sistema biométrico para verificação de autenticidade e outro que compara à informação coletada com um banco de dados a procura de um dado que possa ser igual ao coletado. Para o desenvolvimento do projeto foi necessário, inicialmente, dedicar boa parte do tempo na aquisição de conhecimento das tecnologias e metodologias para a resolução de problemas relacionados à biometria, devido à complexidade do problema. Estas complexidades envolvem as técnicas de processamento de imagens, principalmente a de comparação de imagens biométricas. A outra parte foi dedicada exclusivamente para a implementação do sistema biométrico.

1.2 – OBJETIVO

Neste projeto foi desenvolvido um protótipo de um sistema biométrico de identificação e autenticação de padrões de impressões digitais. Neste protótipo foram utilizados técnicas e métodos amplamente divulgados na literatura, as quais têm a finalidade de localizar e identificar pontos característicos das impressões digitais, facilitando o processo de reconhecimento das mesmas. O desenvolvimento do projeto visou à aquisição de conhecimento sobre importantes técnicas e métodos para processamento de imagens que podem ser utilizadas futuramente em várias outras aplicações. Para o processamento digital de imagens foram utilizados os métodos do domínio espacial, métodos estes que utilizam matrizes denominadas de máscaras.

1.3 – JUSTIFICATIVA

A realização do projeto é justificada pelo fato da biometria ser um ótimo recurso para identificação, apresentando características como universalidade, unicidade, facilidade de coleta e grande aceitação pública. Sendo assim, a utilização das impressões digitais para reconhecimento biométrico oferece segurança, eficácia e comodidade, podendo substituir os métodos convencionais de autenticação ou identificação que são utilizados atualmente.

Outro ponto relevante é que a tecnologia de reconhecimento de indivíduos por comparação de impressão digital é, dentre todas as tecnologias biométricas, a que atualmente oferece a melhor relação custo-benefício.

1.4 – MOTIVAÇÃO

O desenvolvimento deste projeto é motivado, tendo em vista, que a biometria vem para simplificar o processo de identificação de indivíduos, pois dispensa o uso de

cartões, códigos ou qualquer outro recurso no processo de reconhecimento. Além disso, oferece um alto nível de proteção contra diversos tipos de fraudes ao proporcionar o vínculo entre o usuário e o sistema, uma vez que somente o indivíduo em pessoa poderá ser submetido à identificação. Dessa forma, a preocupação com a falsa identificação realizada por terceiros é eliminada, pois a biometria identifica indivíduos através de características únicas pertencentes a cada indivíduo.

1.5 – ESTRUTURA DO TRABALHO

O trabalho está organizado em cinco capítulos conforme descrito a seguir.

O capítulo um apresentou a introdução e descreveu os objetivos e as motivações para o desenvolvimento do trabalho.

O segundo capítulo apresenta a fundamentação teórica básica necessária para compreender conceitos específicos do trabalho onde são abordados assuntos como as técnicas básicas de processamento de imagem.

No capítulo três é feita uma introdução referente à biometria, além de alguns conceitos referentes às impressões digitais e como podem ser classificadas. Neste capítulo são descritas as principais características que possibilitam a comparação entre impressões digitais.

O quarto capítulo é referente ao desenvolvimento do trabalho, onde é apresentada a modelagem do problema bem como a especificação, por meio de diagramas, da implementação do sistema desenvolvido.

Por fim, no capítulo cinco são apresentadas as conclusões do trabalho e sugestões para trabalhos futuros.

2 - FUNDAMENTAÇÃO TEÓRICA BÁSICA

A elaboração do estudo de caso que será responsável pela aplicação dos conceitos obtidos, necessita primeiramente de uma pesquisa teórica com a finalidade de adquirir toda a fundamentação básica que o tema requer. Neste capítulo será feita uma descrição dos assuntos de forma a fornecer toda a base de conhecimento exigida pela área estuda.

2.1 – RECONHECIMENTO DE PADRÕES

O Reconhecimento de Padrões (RP) é a ciência que tem por objetivo a classificação de objetos em categorias ou classes. Desde os primórdios da computação, a tarefa de implementar algoritmos emulando essa capacidade humana, tem se apresentado como uma das mais intrigante e desafiadora (JAIN; DUIN; MAO, 2000). As técnicas de reconhecimento de padrões apresentam um vasto leque de aplicações nas áreas científicas e tecnológicas, principalmente na área de informática. O interesse na área de reconhecimento de padrões tem aumentado recentemente devido a novas aplicações que são não só um desafio, mas também computacionalmente mais exigentes. Estas aplicações incluem *data mining,* ou mineração de dados que identifica um padrão ou uma relação entre milhões de modelos; a classificação de documentos, muito útil para procurar documentos de texto; previsões financeiras; organização e recuperação de bancos de dados multimídia e biometria, que é a identificação pessoal baseada em vários atributos físicos ou comportamentais. A tabela 1 mostra algumas aplicações do reconhecimento de padrões.

Domínio do Problema	Aplicação	Padrão de Entrada	Classes de Padrão
Bioinformática	Análise de Sequência	DNA/Sequência de proteínas	Tipos conhecidos de genes/padrões
Mineração de dados	Busca por padrões significantes	Pontos em um espaço multidimensional	Compactar e bem separar grupos
Classificação de documentos	Busca na Internet	Documento texto	Categorias semânticas (negócios, esportes e etc.)
Análise de documentos de imagem	Máquinas de leitura para cego	Documento de imagem	Palavras e caracteres alfanuméricos
Automação industrial	Inspeção de circuito impresso em placas	Intensidade ou alcance de imagem	Produto defeituoso/não defeituoso
Recuperação de base de dados multimídia	Busca na Internet	Vídeo clipe	Gêneros de vídeos
Reconhecimento biométrico	Identificação pessoal	Face, íris, impressão digital	Usuários autorizados para controle de acesso
Sensoriamento remoto	Prognóstico da produção de colheita	Imagem multiespectral	Categorias de aproveitamento de terra, desenvolvimento de padrões de colheita
Reconhecimento de voz	Inquérito por telefone sem assistência de operador	Voz em forma de onda	Palavras faladas

Tabela 1 – Aplicações do reconhecimento de padrões (JAIN; DUIN; MAO, 2000)

A busca para projetar e construir sistemas capazes de realizar o reconhecimento automático de padrões de forma precisa e confiável é imensamente útil. Durante a resolução dos inúmeros problemas necessários para construir tais sistemas, a compreensão de como é realizado o reconhecimento de padrões no mundo real se faz necessária, pois algumas aplicações como o reconhecimento da fala e o reconhecimento facial, influenciam na maneira como esses sistemas são estruturados.

Existe ainda uma nova aplicação para o reconhecimento de padrão, chamado computação afetiva, que dá a um computador a capacidade de reconhecer e expressar emoções e empregar mecanismos que contribuem para a tomada de decisão racional (JAIN; DUIN; MAO, 2000).

Os seres humanos têm grande facilidade em reconhecer padrões. Sempre que um objeto é observado uma prévia coleta de informações é feita, as quais são comparadas com as informações armazenadas no cérebro relacionadas aquele objeto. A figura 1 ilustra exemplos de padrões.

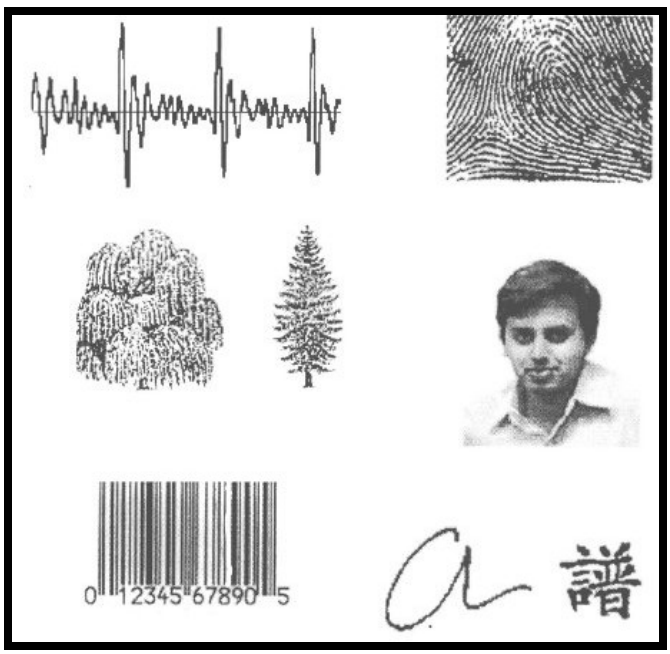

Figura 1 – Exemplos de padrões (PSYCHOLOGY, 2010)

Por meio desta comparação é possível reconhecer o objeto observado. Em um ambiente real, a aplicação deste conceito é simples e familiar para todos, mas implementar o mesmo conceito em um contexto computacional não é uma tarefa fácil. Uma das formas mais simples e relativamente rápida de se obter o reconhecimento é utilizando uma comparação entre modelos. A comparação é utilizada para determinar a similaridade entre as entidades do mesmo tipo (JAIN; DUIN; MAO, 2000).

O processo de comparação é realizado por meio da aquisição de um modelo do que se deseja obter o reconhecimento, que é posteriormente confrontado com o padrão armazenado. No momento da confrontação devem-se levar em conta possíveis translações, rotações ou mudanças de escala que podem ocorrer durante o processo de aquisição. A comparação entre os modelos exige bastante processamento, mas a disponibilidade de processadores mais rápidos a preços acessíveis, tem tornado esta abordagem mais viável.

O desenvolvimento de um sistema biométrico envolve o problema de busca de padrões em imagens. Para obter uma solução razoável é necessário escolher as técnicas e métodos adequados para o problema em questão.

2.2 – PROCESSAMENTO DE IMAGEM

O campo de processamento de imagens está em expansão devido à importância que certas aplicações possuem na vida das pessoas e na sociedade de um modo geral. Esse crescimento também acontece pela grande utilização de imagens e gráficos em uma grande variedade de aplicações em conjunto com o avanço de sistemas de processamento. A necessidade de manipulação e processamento de uma imagem parte do interesse da melhoria das informações obtidas na análise de uma imagem digital, de forma que forneça subsídios para a sua melhor interpretação. Muitas situações exigem o uso de técnicas de processamento de imagens, onde a aplicação de ferramentas matemáticas é fundamental para o sucesso deste tipo de aplicação.

As imagens são produzidas por uma variedade de dispositivos físicos, tais como câmeras de vídeo, equipamentos de radiografia e ressonância magnética, microscópios eletrônicos, radares, equipamento de ultra-som, entre vários outros. A produção e utilização de imagens podem ter diversos objetivos, que vão do puro entretenimento até aplicações militares, médicas ou tecnológicas. O objetivo da análise de imagens, seja por um observador humano ou por uma máquina, é extrair informações úteis e relevantes para cada aplicação desejada. Em geral, a imagem

pura adquirida pelo dispositivo de captura, necessita de transformações e realces que a torne mais adequada para que se possa extrair o conteúdo de informação desejada com maior eficiência.

O Processamento Digital de Imagens (PDI) é uma área da eletrônica/teoria de sinais em que imagens são convertidas em matrizes de números inteiros, sendo que cada elemento desta matriz é composta por um elemento fundamental: o *pixel* (uma abreviação de *Picture Element*). A partir desta matriz de *pixels* que representa a imagem, diversos tipos de processamento digital podem ser implementados por algoritmos computacionais. Na aplicação destes algoritmos são realizadas as transformações necessárias para que se possa, por exemplo, obter uma imagem com os realces pretendidos ou extrair atributos ou informações pertinentes. Assim, o PDI pode ser considerado como a união das áreas de processamento de imagem e visão computacional.

2.2.1 – Representação de Uma Imagem Digital

Uma imagem monocromática é uma função bidimensional *f(x, y)* da intensidade luminosa, onde *x* e *y* denotam coordenadas espaciais, que por convenção: *x = [1, 2,..., M]* e *y = [1, 2,..., N]*. O valor de *f* no ponto *(x, y)* é proporcional ao brilho (ou nível de cinza) da imagem neste ponto, como mostra a figura 2. Esta figura apresenta uma região de 17x17 *pixels* em destaque onde se podem observar os *pixels* e os níveis de cinza ou níveis de luminância de cada um deles. A imagem "*Goldhill*" é frequentemente utilizada para testes e demonstrações em PDI.

Figura 2 – Imagem monocromática "*Goldhill*" (ALBUQUERQUE et al., 2004)

Um *pixel* é o elemento básico em uma imagem. A forma mais comum para o *pixel* é a forma retangular ou quadrada. O *pixel* é também um elemento de dimensões finitas na representação de uma imagem digital.

Para ser analisada computacionalmente, uma imagem monocromática em níveis de cinza deve estar na forma digital, sendo representada pela função de intensidade luminosa *f(x, y)* equivalente ao nível de cinza da imagem em cada ponto num sistema de coordenadas espaciais *(x, y)* que assumem valores inteiros entre 0 e 255. Os níveis de cinza dependem dos valores desses pontos (*pixels*), isto é, valores próximos de 0 representam pontos escuros e valores próximos de 255 os pontos claros. A figura 3 mostra a intensidade dos *pixels* em uma imagem.

218	218	218	165	90	90	90	90	90
218	218	165	165	165	90	90	90	90
218	218	165	165	165	165	90	90	90
218	218	218	218	165	165	165	90	90
218	218	218	218	165	165	165	90	90
218	218	218	218	165	165	165	90	90
218	218	165	165	165	165	90	90	90
218	165	165	165	165	165	90	90	90
165	165	165	165	165	90	90	90	90
165	165	165	90	90	90	90	90	90

Figura 3 – Intensidade dos *pixels*

Frequentemente, a organização de uma imagem sob a forma de uma matriz de *pixels* é feita em uma simetria quadrada. Isto se deve a facilidade de implementação eletrônica, seja dos sistemas de aquisição seja dos sistemas de visualização de imagens. Este tipo de organização provoca o aparecimento de dois problemas importantes nas técnicas de processamento.

Em primeiro lugar um *pixel* não apresenta as mesmas propriedades em todas as direções, isto é, ele é anisotrópico. Esta propriedade faz com que um *pixel* tenha quatro vizinhos de borda e quatro vizinhos de diagonal. Esta propriedade obriga que seja definido o tipo de conectividade que será utilizada. Os tipos de conectividade são: B4 (4-vizinhança) onde considera apenas os vizinhos de borda ou B8 (8-vizinhança) onde considera os vizinhos de borda e os de diagonal. O segundo problema é consequência direta do primeiro, ou seja, as distâncias entre um ponto e seus vizinhos não é a mesma para qualquer tipo de vizinho. Será igual a 1 para vizinhos de borda e $\sqrt{2}$ para aqueles na diagonal. As figuras 4 e 5 mostram esses tipos de conectividade.

- **B4 ou 4-vizinhança**: é definida pelo conjunto dos *pixels* localizados na horizontal e na vertical em relação ao *pixel* central *P*, conforme mostra a figura 4.

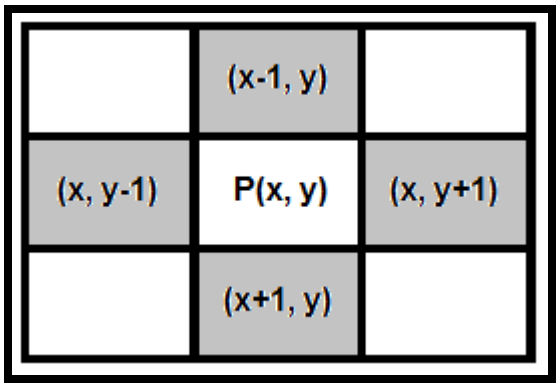

Figura 4 – Representação da 4-vizinhança do *pixel P*

- **B8 ou 8-vizinhança**: é definida pela união do conjunto dos *pixels* localizados na 4-vizinhança com o conjunto dos *pixels* localizados nas diagonais em relação ao *pixel* central *P*, conforme mostra a figura 5.

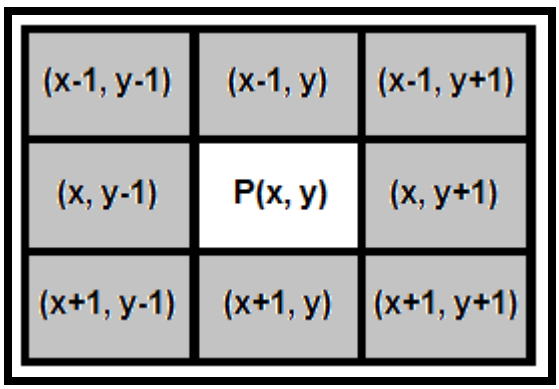

Figura 5 – Representação da 8-vizinhança do *pixel P*

A definição destes tipos de vizinhanças é importante para delimitar a área em que se pretende buscar determinadas características em uma imagem.

2.2.2 – Etapas Para o Processamento Digital de Imagens

Nesta seção serão abordadas as etapas para o processamento digital de imagens. A figura 6 mostra as etapas de um processamento digital de imagens.

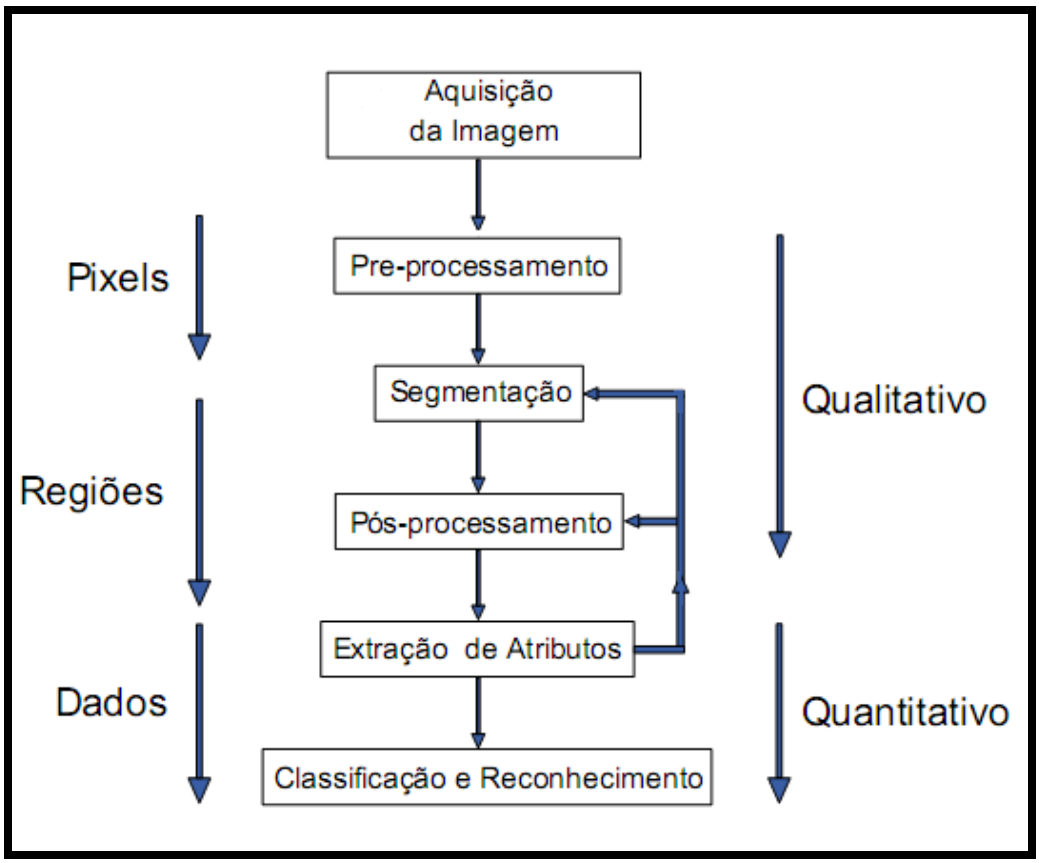

Figura 6 – Etapas de processamento digital de imagens

2.2.2.1 – Aquisição de Imagens

Para obtenção de imagens digitais são necessários dois elementos: dispositivos físicos captadores de imagem e digitalizador. Dispositivos físicos são sensíveis a espectros de energia eletromagnética e o digitalizador converte o sinal elétrico desses dispositivos para o formato digital. Estes elementos são chamados de sistemas de imageamento. O exemplo mais conhecido deste sistema é a câmera

digital, outros são scanners e sensores presentes em satélites. Detalhes sobre aquisição de imagem podem ser vistos em (GONZALES; WOODS, 1992).

2.2.2.2 – Pré-Processamento

As técnicas de pré-processamento têm a função de melhorar a qualidade da imagem. O melhoramento de imagem é obtido através de técnicas, tais como, o melhoramento de contraste e filtragem aplicadas com finalidades específicas, enfatizando características de interesse ou recuperando imagens que sofreram algum tipo de degradação devido à introdução de ruído, perda de contraste ou borramento. A aplicação dessas técnicas, designadas como realce de imagem, são transformações radiométricas que modificam o valor dos níveis de cinza dos pontos da imagem.

2.2.2.2.1 – Melhoramento de Contraste

O melhoramento de contraste busca melhorar a qualidade visual da imagem através da manipulação dos níveis de cinza presentes na imagem. Uma imagem possui valores de intensidade de *pixel*, variando de 0 a 255. Quanto mais espalhados os *pixels* da imagem neste intervalo melhor é o seu contrate. Para (MASCARENHAS; VELASCO, 1989), contraste consiste numa diferença local de luminância e pode ser definido como a razão dos níveis de cinza médios do objeto e do fundo. O processo de melhoramento de contraste transforma a escala de cinza de forma pontual, ou seja, o novo valor do ponto depende somente do valor original do ponto. Uma função de transferência mapeia o valor de um ponto para um novo valor. Essa função é definida pela eq. (1) da seguinte forma:

$$g(x, y) = T(f(x, y)) \quad , \tag{1}$$

onde *f(x, y)* é o valor do nível de cinza original do ponto, *T* é a função de transferência e *g(x, y)* é o novo valor.

Uma boa forma de avaliar o contraste de uma imagem é analisar seu histograma. O histograma de uma imagem monocromática é um gráfico que representa a distribuição dos *pixels* para cada nível de cinza na imagem. O número de *bits* utilizados na representação dos *pixels* influencia na variação de cor que o *pixel* pode ter e consequentemente no comprimento do histograma, de forma que uma imagem de 4 *bits* possui 16 níveis de cinza enquanto uma imagem com 8 *bits* possui 256 tonalidades de cinza diferentes (ROVANI, 2006). No eixo horizontal fica a escala de cinza e no eixo vertical fica a quantidade de *pixels*, conforme ilustrado na figura 7.

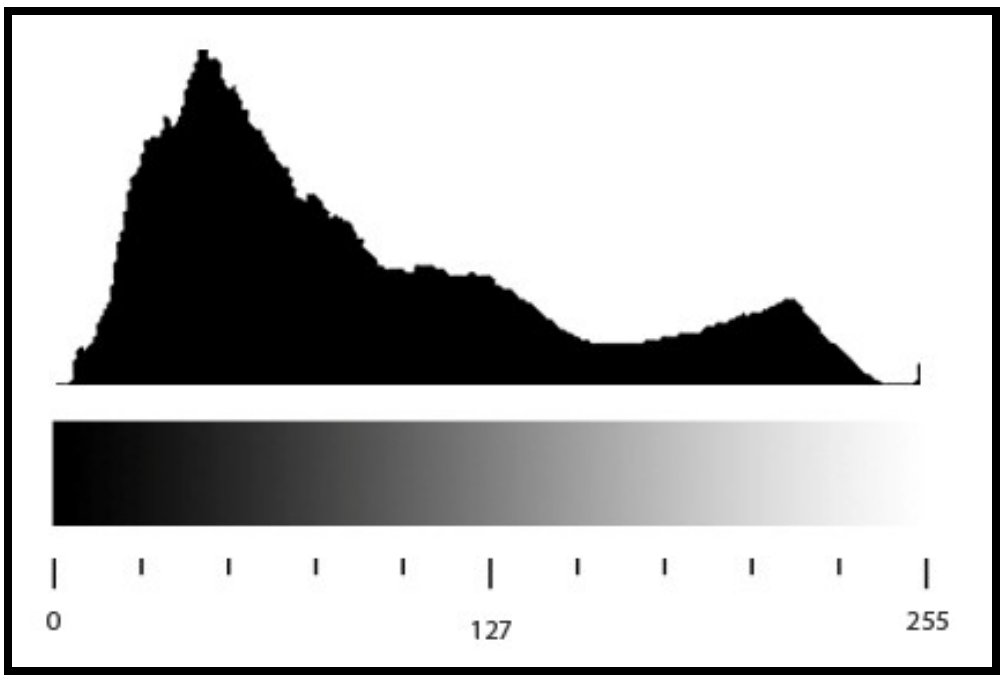

Figura 7 – Histograma (BR, 2010)

O histograma de uma imagem pode ser calculado através da eq. (2) dada por:

$$P_r(r_k) = n_k / n \quad , \tag{2}$$

onde $P_r(r_k)$ é a probabilidade do k-ésimo nível de cinza, n_k é o número de *pixels* cujo nível de cinza corresponde a *k*, *n* é o número total de *pixels* da imagem, $k = 0, 1, ..., L-1$, onde *L* é o número de níveis de cinza da imagem, e $0 \leq r_k \leq 1$ (ROVANI, 2006).

O histograma não preserva a informação espacial da distribuição dos *pixels*, pois este contém apenas a quantidade de *pixels* com um determinado nível de cinza, não a sua posição na imagem. De qualquer forma, o histograma é uma ferramenta importante no processamento de imagens, pois com ele é possível visualizar se uma imagem apresenta um bom contraste, se está escura demais ou muito clara ou ainda ser utilizado no processo de binarização, quando a imagem apresentar as características apropriadas.

2.2.2.2.2 – Filtragem

As técnicas de filtragem são transformações da imagem *pixel* a *pixel*, que não dependem apenas do nível de cinza de um determinado *pixel*, mas também do valor dos níveis de cinza dos *pixels* vizinhos. O processo de filtragem é feito utilizando matrizes denominadas máscaras, as quais são aplicadas sobre a imagem. A figura 8 mostra o processo de filtragem de uma imagem.

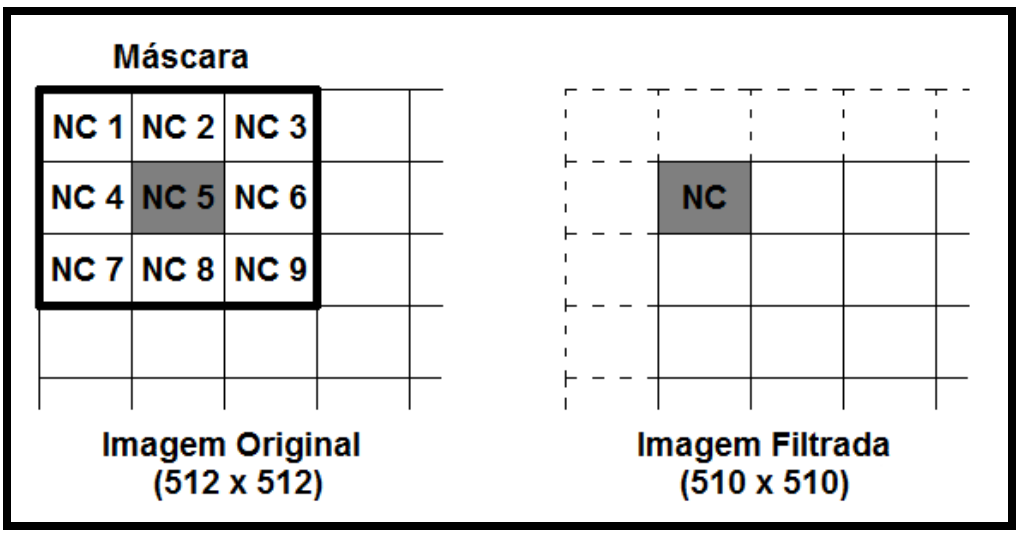

Figura 8 – Processo de filtragem de uma imagem (ALBUQUERQUE et al., 2004)

A aplicação da máscara com centro na posição (*i, j*), sendo *i* o número de uma dada linha e *j* o número de uma dada coluna sobre a imagem, consiste na substituição do valor do *pixel* na posição (*i, j*) por um novo valor que depende dos valores dos *pixels* vizinhos e dos pesos da máscara, gerando uma nova imagem, com a eliminação das linhas e colunas iniciais e finais da imagem original, em que se pretende buscar determinadas características. O processo de filtragem procura extrair informações inseridas pelo processo de imageamento ou durante a transmissão da imagem. Os principais objetivos da filtragem são:

- Melhorar a qualidade de uma imagem (*realce-sharpening-enhancement*);
- Eliminar ruídos (*noise*);
- Corrigir imagens;
- Eliminar ou provocar “distorções”;
- Criar efeitos artísticos.

Um dos principais problemas encontrados no processamento de imagens é a presença de ruídos. Esses ruídos podem ser gerados durante o processo de aquisição da imagem. Um tipo muito comum de ruído gerado principalmente por equipamentos eletrônicos é o *salt and pepper* (sal e pimenta) que se manifesta em uma imagem como pontos pretos em regiões brancas ou pontos brancos em áreas escuras. Os filtros são divididos em duas categorias: filtros no domínio da frequência (utilização da transformada de Fourier e baseadas no teorema da convolução) e filtros no domínio espacial (utilização de máscaras).

Técnicas de processamento no domínio espacial são baseadas em filtros que manipulam o plano da imagem, enquanto que as técnicas de processamento no domínio da frequência são baseadas em filtros que agem sobre o espectro da imagem. É comum, para realçar determinadas características de uma imagem, combinar vários métodos que estejam baseados nestas duas categorias.

- **Filtros no Domínio da Frequência**

Estes filtros operam utilizando métodos que são comumente chamados de transformadas. Uma das ferramentas utilizada neste processamento é a transformada de Fourier, a qual nos permite ter uma visão da imagem a ser analisada no domínio da frequência, facilitando sobremaneira esta análise e o seu processamento. Na prática, a utilização de algoritmos para execução rápida das transformadas de Fourier (*Fast Fourier Transform* - FFT) juntamente com os teoremas de convolução e da correlação permitem, de maneira simplificada, a implementação das técnicas de filtragens para eliminação de ruídos e interferências das imagens (ou de uma maneira geral, sinais) em análise. Neste projeto não serão utilizados os filtros no domínio da frequência. Detalhes sobre filtragem no domínio da frequência podem ser encontradas em (GONZALES; WOODS,1992).

- **Filtros no Domínio do Espaço**

A filtragem no espaço é considerada uma operação local, ou seja, o nível de cinza de um ponto depende do original e de sua vizinhança. O princípio de funcionamento de tal filtro está baseado em máscaras de deslocamento as quais são matrizes com pesos associados em cada posição. A máscara com centro na posição *(x, y)* é colocada sobre o *pixel* a ser modificado na imagem. O *pixel* correspondente na imagem é substituído por um valor que considera os *pixels* vizinhos e os pesos correspondentes na máscara. A soma de todos os produtos dos pesos da máscara pelos *pixels* correspondente na imagem resulta em um novo valor de cinza que substituirá o *pixel* central.

Neste projeto será utilizada somente a filtragem no domínio espacial e, para isso, será feita uma descrição mais detalhada desta técnica.

A filtragem no domínio espacial é um procedimento executado diretamente sobre o conjunto de *pixels* que compõem uma imagem, podendo ser expresso pela eq. (3):

$$g(x_i, y_i) = T[f(x_i, y_i)] \quad , \qquad (3)$$

onde $f(x_i, y_i)$ é a imagem de entrada, $g(x_i, y_i)$ é a imagem processada e T é um operador sobre f, definido sobre o *pixel* (x_i, y_i) e alguns *pixels* vizinhos. Esta equação é semelhante à função de transparência dada pela eq. (1).

O processo de filtragem é baseado na utilização de máscaras, as quais são matrizes, normalmente 3x3 ou 5x5, sendo que a distribuição de valores nessa máscara define o tipo de filtragem a ser executada durante o processamento (DEKKER, 2002). A filtragem no domínio espacial pode ser considerada uma operação local, uma vez que o nível de cinza de um *pixel* depende somente do seu valor original e dos valores dos *pixels* em sua vizinhança.

O uso de máscaras sobre as imagens no domínio espacial é usualmente chamado de filtragem espacial e as máscaras são chamadas de filtros espaciais. Os filtros da média e da mediana são exemplos de filtros utilizados para essa finalidade. O filtro da média suaviza o ruído, porém pode borrar a imagem, uma vez que ocorre uma perda de detalhes se o *pixel* que for alterado variar significantemente do valor original. O filtro da mediana, por sua vez, é mais eficiente, pois preserva o contorno e pequenos detalhes da imagem.

- ***Filtro da Média***

Um dos filtros mais simples que pode ser definido no domínio espacial é o filtro da média, onde o valor da função $g(x, y)$, que representa a imagem após a aplicação do filtro, é definido pela média aritmética de todos os pontos pertencentes à vizinhança de cada *pixel* da imagem original. A figura 9 representa uma imagem em níveis de cinza com a aplicação do filtro da média.

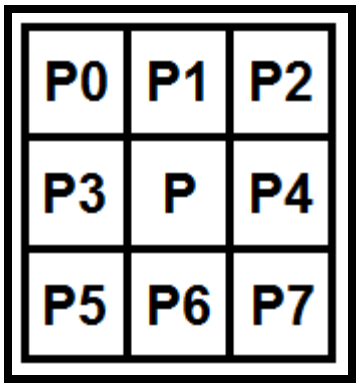

Figura 9 – Aplicação do filtro da média

O novo valor para o *pixel* central *P* após a aplicação do filtro da média utilizando uma janela 3x3 é dada pela eq. (4):

$$P = \frac{P0+P1+P2+P3+P+P4+P5+P6+P7}{9}\ , \qquad (4)$$

Como o valor de um *pixel* deve ser inteiro, o resultado é então arredondado. Dessa forma, a filtragem ocorre pela aplicação de uma janela que percorre toda a imagem e o *pixel* central dessa janela recebe a média aritmética dos *pixels* vizinhos dentro dessa área. Por isso, apesar de conseguir diminuir o ruído, o filtro apresenta bons resultados apenas em regiões homogêneas, uma vez que produz uma desfocalização que varia de acordo com as dimensões da janela utilizada, de forma que quanto maior a dimensão, maior a desfocalização decorrente da diversidade de valores que pode haver na vizinhança do *pixel* (FARIA, 2005).

Por ser uma técnica simples, o filtro da média é útil e relativamente rápida de ser aplicada, uma vez que não necessita de processamento complexo, apenas somas e divisões. Contudo, o filtro da média apresenta uma grande perda nos detalhes da imagem, dando o efeito de borramento.

o ***Filtro da Mediana***

O filtro da mediana, assim como o filtro da média, consiste em substituir o valor de cada *pixel* da imagem original observando os valores dos *pixels* vizinhos. Os valores dos *pixels* da vizinhança são ordenados e o valor da mediana é atribuído ao *pixel* que está sendo processado. A mediana de um conjunto de *n* valores é obtida da seguinte forma:

- Se *n* for ímpar, o resultado é o elemento central da lista ordenada com os valores dos *pixels*;
- Se *n* for par, a mediana é a média dos valores dos dois *pixels* nas posições centrais da lista ordenada com os valores dos *pixels*.

A figura 10 representa uma janela 3x3 sobre uma imagem e seus respectivos níveis de cinza com a aplicação do filtro da mediana.

45	130	143
50	137	127
56	125	139

Figura 10 – Aplicação do filtro da mediana

O Conjunto Ordenado (CO) de *pixels* que compõe a janela é dado pela eq. (5):

$$CO = \{45, 50, 56, 125, 127, 130, 137, 139, 143\} \quad , \tag{5}$$

onde o quinto elemento é o valor da mediana, uma vez que o número total de elementos do conjunto é ímpar. Dessa forma, o valor em nível de cinza do *pixel* central mudará de 137 para 127.

O filtro da mediana é mais eficiente para eliminar ruídos do tipo “sal e pimenta” (chuviscos), retendo os detalhes da imagem, porque eles não dependem dos valores que são significativamente diferentes dos valores típicos em uma vizinhança, uma vez que o valor atribuído ao *pixel* processado é o mesmo valor de um de seus vizinhos (FARIA, 2005).

Uma de suas vantagens é manter os principais detalhes da imagem, ao contrário do filtro de média. A desvantagem é que o seu algoritmo é mais complexo, visto que utiliza ordenamento de valores para obter o resultado (MARION, 1991). Entretanto, sua aplicação suaviza a imagem preservando a informação de bordas e outros detalhes da imagem.

- ***Filtro de Contraste***

A aplicação de um filtro de contraste em imagens digitais tem como objetivo aumentar a distinção e melhorar os aspectos visuais entre os objetos nelas contidos. Uma forma de alcançar este objetivo é calcular para cada *pixel* um valor médio de intensidade em uma vizinhança 5x5. Se o valor do *pixel* for menor que a média do bloco considerado, o *pixel* processado recebe valor zero, caso contrário, mantém seu valor original (COSTA, 2001). O filtro de contraste é expresso pela eq. (6):

$$g(x, y) = \begin{cases} 0, \text{ se } f(x, y) < M \\ f(x, y), \text{ se } f(x, y) \geq M \end{cases} \quad , \tag{6}$$

onde *f*(*x*, *y*) é o *pixel* processado na imagem de entrada, *g*(*x*, *y*) é o valor para o *pixel* processado na imagem filtrada e *M* é a média de valores dos *pixels* em uma vizinhança 5x5 de *f(x, y)*.

O aumento de contraste realça detalhes que tenham sidos borrados em uma imagem, como consequência de erros ou como efeito natural de um método de aquisição. Quanto menos borrada a imagem mais detalhes serão preservados (FARIA, 2005).

2.2.2.3 – Segmentação

A segmentação se refere ao processo de dividir uma imagem digital em múltiplas regiões (conjunto de *pixels*) ou objetos, com o objetivo de simplificar e/ou mudar a representação de uma imagem facilitando sua análise. Segmentação de imagens é tipicamente usada para localizar objetos e formas (linhas, curvas, etc) em imagens.

É usual denominar “objetos” da imagem os grupos de *pixels* de interesse, ou que fornecem alguma informação para o processamento digital de imagem. Da mesma forma que a denominação “fundo” da imagem é utilizada para o grupo de *pixels* que podem ser desprezados ou que não têm utilidade no PDI. Essas denominações “objeto” e “fundo” possuem uma conotação bastante subjetiva, podendo se referir a grupos de *pixels* que formam determinadas regiões na imagem sem que representem um objeto, de modo literal, presente na imagem processada.

Os tipos de segmentação existentes são:

- **Baseadas em formatos**
  - Detecção de descontinuidades;
  - Detecção de pontos;
  - Detecção de linhas;

- Detecção de bordas.

- **Baseadas em características dos *pixels***
  - Segmentação de cores;
  - Segmentação de intensidade.

A segmentação é considerada, dentre todas as etapas do processamento de imagens, a etapa mais crítica do tratamento da informação. Nesta etapa de segmentação é que são definidas as regiões de interesse para processamento e análise posteriores. Como consequência deste fato, quaisquer erros ou distorções presentes nestas etapas se refletem nas demais etapas, de forma a produzir ao final do processo, resultados não desejados que possam contribuir de forma negativa para a eficiência de todo o processamento.

Deve ser ressaltado que não existe um modelo formal para a segmentação de imagens. A segmentação é um processo empírico e adaptativo, procurando sempre se adequar às características particulares de cada tipo de imagem e aos objetivos que se pretende alcançar.

De um modo geral, as técnicas de segmentação utilizam duas abordagens principais: a similaridade entre os *pixels* e a descontinuidade entre eles. Sem dúvida, a técnica baseada em similaridade mais utilizada é a chamada binarização. A binarização de imagens ou *image thresholding* é uma técnica eficiente e simples do ponto de vista computacional, sendo, portanto, largamente utilizada em sistemas de visão computacional. Este tipo de segmentação é utilizado quando as amplitudes dos níveis de cinzas são suficientes para caracterizar os “objetos” presentes na imagem. Na binarização, um nível de cinza é considerado como um limiar de separação entre os *pixels* que compõem os objetos e o fundo. Nesta técnica, se obtém como saída do sistema uma imagem binária, isto é, uma imagem com apenas dois níveis de luminância: preto e branco. A determinação deste limiar de modo otimizado para segmentação da imagem é o objetivo principal dos diversos métodos

de binarização existentes. As técnicas baseadas em descontinuidade entre os *pixels procuram* determinar variações abruptas do nível de luminância entre *pixels* vizinhos. Estas variações, em geral, permitem detectar o grupo de *pixels* que delimitam os contornos ou bordas dos objetos na imagem. A técnica de segmentação baseada em descontinuidade mais utilizada é a chamada detecção de bordas.

2.2.2.3.1 – Binarização

A binarização ou limiarização é o método mais simples e uma das mais importantes abordagens para a realização da segmentação de imagens (FARIA, 2005). Resumidamente, consiste em separar uma imagem em regiões de interesse e não interesse, representadas por *pixels* pretos e brancos.

A conversão de uma imagem em níveis de cinza para uma imagem binária, com somente dois tons, é necessária em várias aplicações que envolvem o processamento de imagem. Essa conversão é feita por meio do processo de binarização que verifica a intensidade dos *pixels* para decidir se ele receberá valor 0 correspondente a preto ou 1 correspondente a branco.

Uma comparação é feita entre valor do *pixel* e um limiar chamado de nível de *threshold* para estabelecer qual dos dois valores será atribuído ao *pixel*, de forma que se o valor do *pixel* for menor ou igual ao nível de *threshold,* o valor atribuído é 0, caso contrário é atribuído ao *pixel* o valor 1 (FARIA, 2005). A operação de binarização pode ser expressa pela eq. (7):

$$g(x, y) = \begin{cases} 0, \text{ se } f(x, y) \leq T \\ 1, \text{ se } f(x, y) > T \end{cases}, \qquad (7)$$

onde *f*(*x*, *y*) é o *pixel* processado na imagem de entrada, *g*(*x*, *y*) é o valor para o *pixel* processado na imagem binária resultante e *T* é o valor do nível de *threshold*.

A imagem resultante do processo de binarização é uma imagem segmentada, onde os *pixels* com valor 0 ou pretos correspondem aos objetos e aqueles com o valor 1 ou brancos formam o fundo da imagem. A escolha do *threshold* é muito importante para o sucesso da binarização, por isso deve ser feita com o cuidado para que não capture imagens que não façam parte do objeto de interesse ou para que não ocorra à perda de informações relevantes.

O método utilizado na definição do limiar determina o tipo de binarização aplicada, sendo que esta pode ser de duas formas: pela análise da imagem como um todo, onde um único limiar é utilizado para toda a imagem (binarização global); ou através da análise de regiões ou blocos da imagem, onde cada bloco tem um limiar específico (binarização local).

- **Binarização Global**

Na binarização global um mesmo valor de *threshold* é utilizado em toda a extensão da imagem. O histograma da imagem pode auxiliar na escolha deste ponto de corte, pois a observação dele permite localizar o melhor valor de *T* para a imagem, de forma que quanto mais bimodal for o histograma, mais fácil à localização do valor de *threshold*. Quando a imagem é composta por um objeto e um fundo é possível estabelecer o ponto de corte através de um isolamento das regiões que representem o fundo e o objeto (FARIA, 2005).

Uma imagem com fundo e objeto bem distintos, cujos níveis de cinza possuem uma variação bem definida, apresenta um histograma com dois picos bem distintos separados por um vale de valores relativamente baixos, conforme ilustrado na figura 11. Neste caso, a binarização geralmente é realizada através do histograma da imagem, ou seja, é utilizada a bipartição do histograma para definir o valor de *T*.

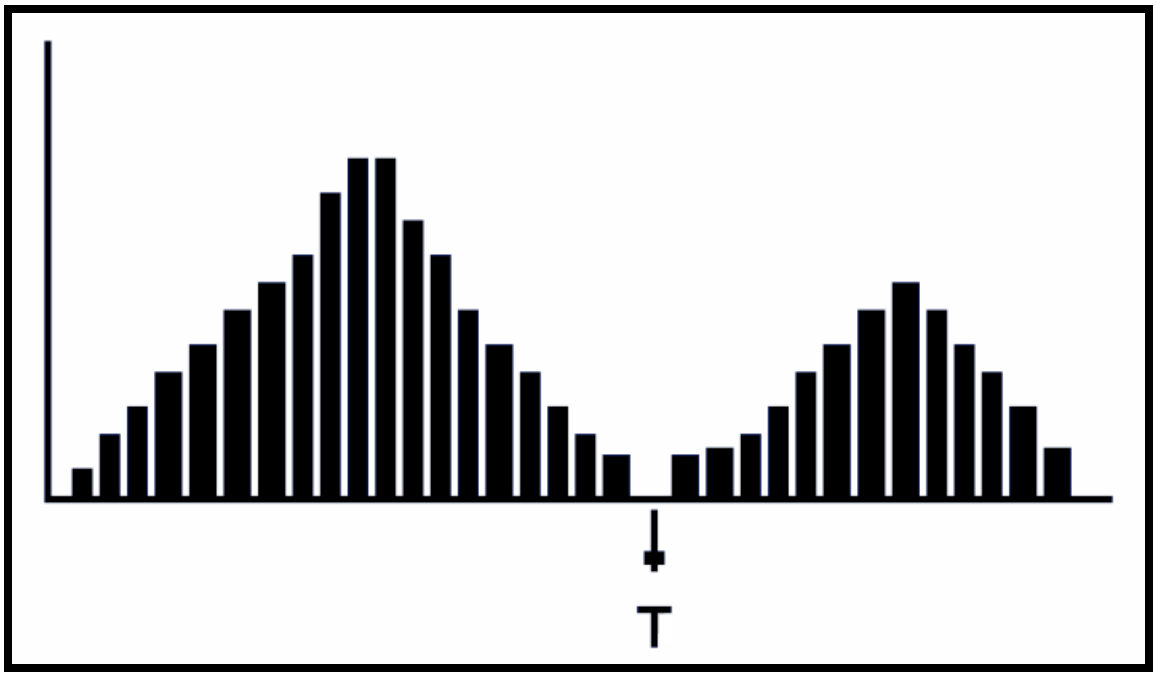

Figura 11 – Histograma biparticionado (Faria, 2005)

Em alguns casos, no entanto, não se consegue apenas um limiar que resulte em uma boa segmentação para toda a imagem. Para esses casos pode ser utilizada a técnica de binarização local.

- **Binarização Local**

Quando uma imagem apresenta vários objetos de modo que o valor de cinza não é o mesmo em diferentes partes da imagem, torna-se necessário o cálculo de um limiar específico para cada região, caracterizando assim uma binarização local.

Neste caso, a operação de *threshold* deve ser aplicada usando pequenos blocos de tamanho 3x3, 5x5, 7x7 entre outros tamanhos. Uma forma relativamente simples de aplicação da binarização local é utilizar o valor médio de cinza do bloco considerado como valor de nível de *threshold* (Costa, 2001).

Outro exemplo de binarização local é o método de Bernsen, o qual consiste, assim como o método anterior, em percorrer uma vizinhança de dimensão 3x3, 5x5 entre

outros, sendo que o limiar é escolhido como o um valor intermediário, que é a média entre o mínimo e o máximo tom de cinza da vizinhança do *pixel*, conforme expresso na eq. (8):

$$T = \frac{Zmin + Zmax}{2}, \tag{8}$$

onde *Zmin* e *Zmax* são respectivamente, os níveis mínimo e máximo de cinza encontrado no bloco considerado (FARIA, 2005).

Portanto, na binarização local, para cada região da imagem é calculado um limiar e em seguida uma comparação é realizada entre o nível de *threshold* calculado e os *pixels* localizados no bloco analisado. Se o *pixel* comparado for maior que o limiar, então é atribuído a este *pixel* o valor 1, caso contrário o *pixel* recebe o valor 0.

2.2.2.3.2 – Afinamento

Ao digitalizar uma imagem, é preferível utilizar uma resolução alta para assegurar que nenhuma informação indispensável seja perdida durante a digitalização. Deste modo, as linhas que constituem a imagem apresentam vários *pixels* de largura. O processo de afinamento ou esqueletização, também conhecido como *thinning*, consiste em minimizar a quantidade de pontos da imagem sem afetar sua forma original.

A principal característica da técnica de *thinning* é reduzir uma imagem a uma fina linha representativa por meio da eliminação de informações de espessura. Dessa forma, a quantidade de dados na imagem é reduzida possibilitando uma análise estrutural simples através de uma representação simplificada dos objetos contidos na mesma. Esta redução transforma os traços da imagem a um *pixel* de largura, de forma que a estrutura do objeto seja preservada (MORGAN, 2008).

O algoritmo de afinamento exclui, de forma sucessiva, as camadas da extremidade da borda dos traços até que permaneça somente o esqueleto da imagem com espessura de um *pixel* apenas. A exclusão de um *pixel* depende de seus vizinhos, sendo que a forma como estes são examinados classifica os algoritmos como sequenciais ou paralelos.

Nos algoritmos sequenciais a exclusão é feita examinando os *pixels* em uma sequência fixa a cada iteração, sendo que a exclusão do *pixel* na n-ésima iteração depende de todas as operações que tenham sido realizadas até o momento, ou seja, do resultado da (n-1)-ésima iteração, assim como os *pixels* já processados na n-ésima iteração. Em contra partida, nos algoritmos paralelos a exclusão na n-ésima iteração depende apenas dos *pixels* da iteração *n-1*, assim todos os *pixels* podem ser analisados de forma independente e paralela a cada iteração (MORGAN, 2008).

Algoritmos sequenciais geram esqueletos melhores, contudo exigem muito tempo de processamento. Já os algoritmos paralelos caracterizam-se pela velocidade, mas muitas vezes originam esqueletos com falhas.

- **Método Zhang-Suen**

Um método muito utilizado para afinamento de imagens é o método Zhang-Suen, cuja idéia básica é decidir se um determinado *pixel* será eliminado verificando os oito *pixels* que pertencem a sua vizinhança (FARIA, 2005). O algoritmo de Zhang-Suen é um algoritmo paralelo rápido e eficiente que mantém a conectividade dos objetos nos esqueletos gerados. Teve seus estudos iniciados por volta de 1984 obtendo resultados superiores a outros da época. Entretanto, muitas melhorias foram propostas por pesquisadores melhorando ainda mais o algoritmo que ainda hoje é muito utilizado (MORGAN, 2008).

Cada *pixel* da imagem original que representa o objeto é analisado com o intuito de determina se o *pixel* será ou não removido, ou seja, se ele é um *pixel* redundante. Existem quatro regras que devem ser aplicadas e, se e somente se as quatro forem

satisfeitas o *pixel* poderá ser eliminado. A decisão é tomada avaliando o *pixel P* e seus 8-vizinhos que são numerados em sentido horário, conforme mostrado na figura 12.

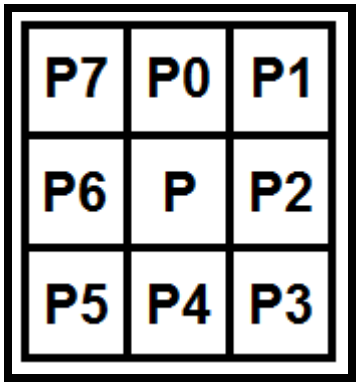

Figura 12 – Numeração dos 8-vizinhos

O algoritmo de Zhang-Suen é dividido em duas iterações em que um *pixel P* é apagado se todas as seguintes condições forem verdadeiras (DEKKER, 2002):

- **Condições da iteração 1**:
  a) $2 \leq N(p) \leq 6$
  b) $S(p) = 1$
  c) $P0 + P2 + P4 = 1$
  d) $P2 + P4 + P6 = 1$
- **Condições da iteração 2:**
  a) $2 \leq N(p) \leq 6$
  b) $S(p) = 1$
  c) $P0 + P2 + P6 = 1$
  d) $P0 + P4 + P6 = 1$

Tanto na primeira como na segunda iteração as condições (a) e (b) são as mesmas. A condição (a) verifica se existem ao menos dois *pixels* vizinhos pretos e não mais do que seis. O número de vizinhos se refere aos *pixels* na faixa *P0, P1, ... , P7* que não fazem parte do fundo da imagem. A figura 13 mostra a esquerda um *pixel* com 2 vizinhos pretos e outro a direita que apresenta 6 vizinhos pretos.

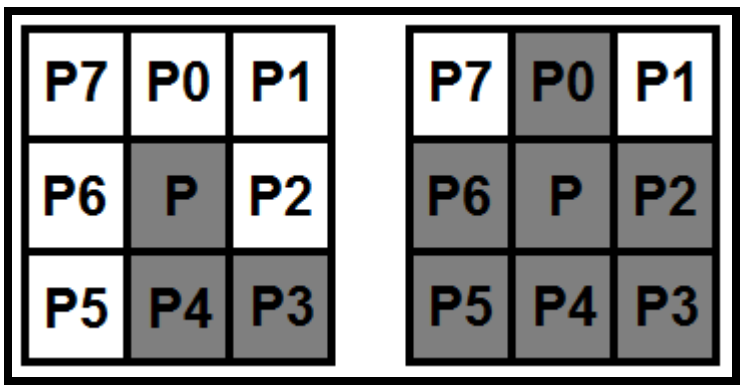

Figura 13 – Vizinhos pretos do *pixel P*

A condição (b) verifica se o número de conectividade do *pixel P* é 1. O número de conectividade é definido como sendo o número de transições de branco para preto nos *pixels* quando estes são visitados em ordem (*P0, P1, ... , P7, P0*) ao redor do *pixel* central *P,* que deve ser exclusivamente 1. A figura 14 mostra a esquerda um *pixel* com conectividade 1 e outro a direita que apresenta conectividade 2.

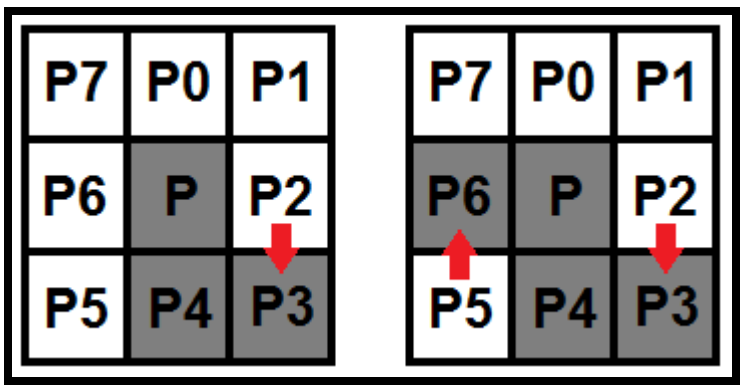

Figura 14 – Conectividade do *pixel P*

As condições (c) e (d) são diferentes em cada iteração. Na primeira iteração a condição (c) verifica se ao menos um dos *pixels P0, P2, P4* são brancos, da mesma forma a condição (d) verifica se ao menos um dos *pixels P2, P4, P6* são brancos. Na segunda iteração acontece o mesmo, porém a condição (c) verifica se ao menos um dos *pixels P0, P2, P6* são brancos e a condição (d) verifica se ao menos um dos *pixels P0, P4, P6* são brancos.

A figura 15 mostra um *pixel* que deve ser excluído independente da iteração, pois todas as condições são verdadeiras.

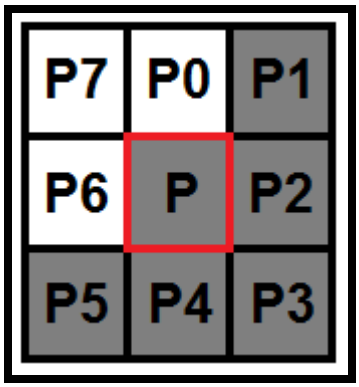

Figura 15 – *Pixel* marcado para exclusão

É importante ressaltar que em ambas as iterações, os *pixels* só devem ser eliminados no final da iteração. Dessa forma, a primeira iteração é executada e a cada *pixel* localizado que estiver de acordo com as condições referentes à primeira iteração é marcado para exclusão, porém somente no final desta iteração todos os *pixels* que foram marcados são excluídos, ou seja, recebem o valor 1 referente a branco e passam a fazer parte do fundo da imagem. Em seguida, acontece o mesmo para a segunda iteração. Se no final da segunda iteração não existirem *pixels* para serem eliminados, então a esqueletização está completa, caso contrário o processo é repetido a partir da primeira iteração passando também pela segunda.

- **Limpeza do Esqueleto**

Após o processo de afinamento a imagem é composta por linhas que apresentam a espessura de apenas um *pixel*. Entretanto, alguns pontos apresentam forma semelhante a uma escada, cuja remoção não afeta o formato nem a conectividade do objeto. Dessa forma, é possível realizar uma limpeza do esqueleto através da aplicação de um processo de remoção de serrilhamento (*staircase removal*), o qual consiste na seguinte observação: metade dos pontos que apresentam uma forma semelhante a uma escada pode ser removida sem afetar o formato ou a conectividade do objeto (FARIA, 2005).

As máscaras mostradas na figura 16 são aplicadas em toda imagem já afinada, de forma que se o *pixel* central de uma das máscaras pertencer ao objeto, ou seja, apresentar valor 0 referente a preto, ele pode ser removido se um dos valores *X* da referida máscara for 1, ou seja, branco.

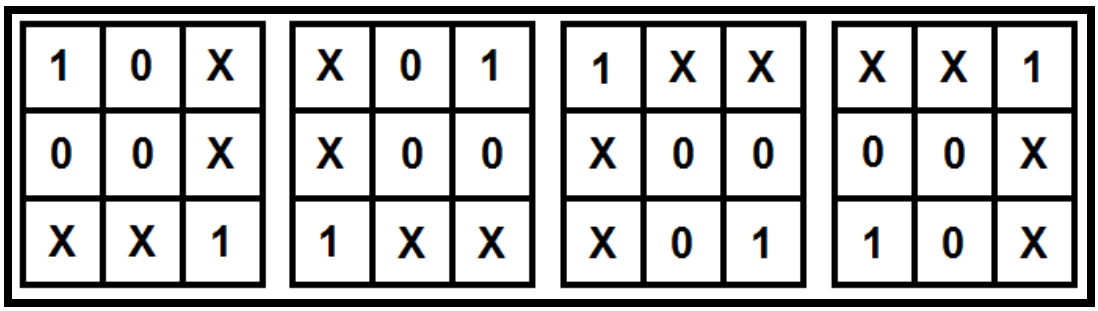

Figura 16 – Máscaras para limpeza do esqueleto (FARIA, 2005)

2.2.2.4 – Pós-Processamento

O pós-processamento geralmente é a etapa que sucede a segmentação. É nesta etapa que os principais defeitos ou imperfeições da segmentação são devidamente corrigidos. Normalmente, estes defeitos da segmentação são corrigidos através de

técnicas de Morfologia Matemática, com a aplicação em sequência de filtros morfológicos que realizam uma análise quantitativa dos *pixels* da imagem.

2.2.2.4.1 – Operações Morfológicas Básicas

A Morfologia Matemática (MM) é uma das grandes áreas do processamento digital de imagens. Todos os métodos descritos pela MM são fundamentalmente baseados em duas linhas: os operadores booleanos de conjuntos (união, interseção, complemento, etc.) e a noção de forma básica, chamado de “elemento estruturante”. As operações são realizadas sempre entre a imagem e o elemento estruturante. A forma do elemento estruturante é em função do tratamento desejado e do tipo de conectividade adotada (B4 ou B8). Dois operadores básicos são utilizados na maior parte das técnicas de MM: a erosão e a dilatação.

- **Operação de Erosão**

A operação de erosão consiste em eliminar do conjunto *X* os *pixels x* em função do elemento estruturante *B*, conforme eq. (9):

$$Y = E^{B}(X) \rightarrow Y = \{x/B(x) \subset X\} \quad , \tag{9}$$

onde *B(x)* é o elemento estruturante centrado no *pixel x*. Na prática, este procedimento corresponde a construir um novo conjunto de pontos *Y*, a partir do conjunto *X*, tal que o elemento estruturante esteja inserido totalmente em *X*.

- **Operação de Dilatação**

A operação dilatação consiste em dilatar o objeto *X* como elemento estruturante *B*, conforme eq.(10):

$$Y = D^B(X) \rightarrow Y = (E^B(X^c))^c = \{x/B(x) \cap \subset X \neq 0\} \quad , \tag{10}$$

onde *c* representa o complemento da operação booleana.

A figura 17 mostra um objeto *X* como um grupo de *pixels x* delimitado por uma linha tracejada, onde se obtém a forma *Y*. Observe que *x1* é um ponto de *X* que também pertence a *Y*. Em (a) *x2* pertence a *X*, mas não a *Y* devido à operação de erosão. Por outro lado, em (b) *x2* passa a pertencer a *Y* devido à dilatação. Observe que *x3* não pertence a ambos *X* e *Y*.

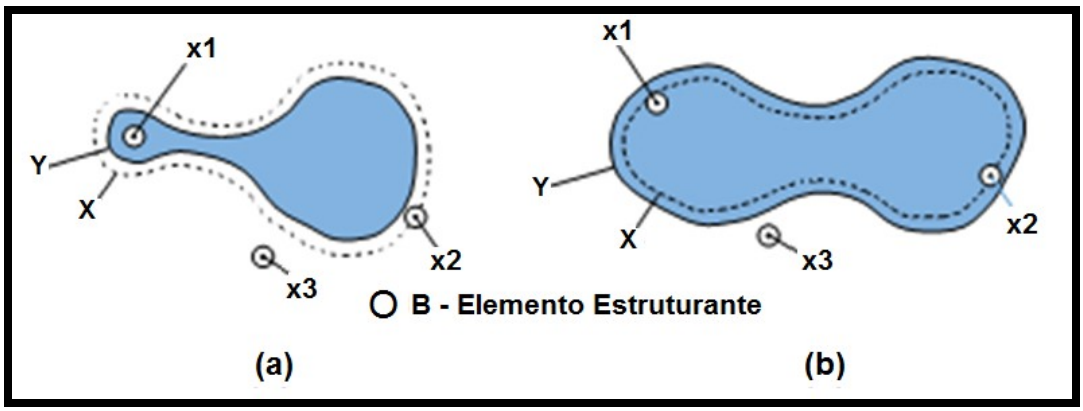

Figura 17 – Operação de erosão (a) e dilatação (b) (ALBUQUERQUE et al., 2004)

2.2.2.5 – Extração de Atributos

A etapa final de um sistema de processamento de imagens é aquela em que se extraem as informações úteis da imagem. Quando o objetivo do processamento é obter informações numéricas, realiza-se a extração de atributos da imagem.

2.2.2.5.1 – Rotulação ou Labelização

A etapa chamada Labelização ou Rotulação é uma etapa intermediária na extração de atributos. Após a etapa de segmentação, obtém se uma imagem onde as regiões correspondentes aos “objetos” estão separadas daquelas correspondentes ao “fundo” da imagem. Neste ponto do sistema de processamento, as regiões de interesse estão agrupadas por *pixels* que se tocam. O próximo passo é dar um rótulo (ou *label*) para cada um desses grupos de *pixels*. Esta identificação permitirá posteriormente parametrizar os objetos segmentados calculando para cada região de *pixels* contíguos um parâmetro específico, como área ou perímetro. A etapa de “labelização” cria um rótulo que identifica cada uma dessas regiões para que os processos seguintes de tratamento da informação sejam concentrados em cada uma das regiões que receberam um rótulo. A figura 18 apresenta um exemplo desta técnica para uma imagem constituída de células bem delimitadas entre si, onde (a) ilustra a imagem original composta por regiões contíguas de *pixels* e (b) a imagem final após o processo de rotulação. As cores são utilizadas para auxiliar na visualização das regiões.

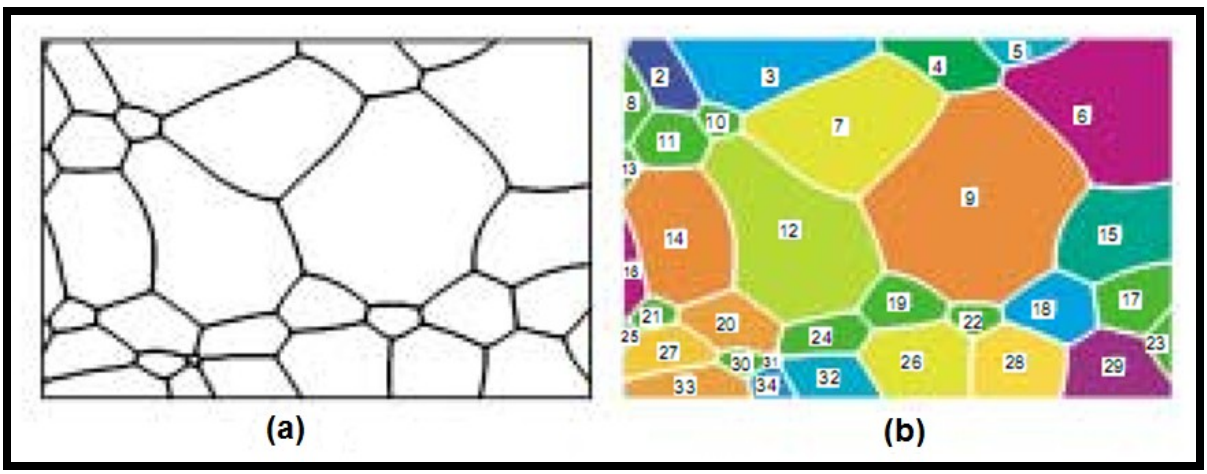

Figura 18 – (a) imagem original e (b) imagem rotulada (ALBUQUERQUE et al., 2004)

2.2.2.6 – Classificação e Reconhecimento

O objetivo do reconhecimento é realizar, de forma automática, a “identificação” dos objetos segmentados na imagem. Existem duas etapas no processo e classificação de formas: o aprendizado e o reconhecimento propriamente dito. Na maior parte dos sistemas de reconhecimento de formas, os parâmetros provenientes da etapa de extração de atributos são utilizados para construir um espaço de medida à *N* dimensões. Os sistemas de aprendizado irão definir uma função discriminante que separe eficientemente todas as formas representadas neste espaço de medida.

Os processos de aprendizado podem ser divididos em dois tipos: os métodos supervisionados e não supervisionados. No método supervisionado, o classificador, em sua fase de aprendizado, recebe informações de como as classes devem ser identificadas. Este processo pode ser lento e de elevado custo computacional. No caso em que a classificação não é supervisionada, o classificador receberá os objetos desconhecidos e, a partir da medida dos diferentes parâmetros (atributos dos objetos presentes na imagem), ele será alocado em diferentes classes. A identificação de classes é usualmente realizada a partir da identificação de agrupamentos em “*clusters*” de objetos no espaço de medidas.

2.3 – LINGUAGEM JAVA

Java é uma linguagem de programação orientada a objeto, desenvolvida na década de 90 pelo programador James Gosling, da empresa Sun Microsystems. Diferentemente das linguagens convencionais, que são compiladas para código nativo, a linguagem Java é compilada para um “*bytecode*” que é interpretado e executado por uma máquina virtual, a *Java Virtual Machine* (JVM).

2.3.1 – Características

A linguagem Java foi projetada tendo em vista os seguintes objetivos:

- **Orientação a Objeto**: baseado no modelo de Smalltalk e Simula67;
- **Portabilidade**: independência de plataforma;
- **Recursos de Rede**: possui extensa biblioteca de rotinas que facilitam a cooperação com protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*), como HTTP (*Hypertext Transfer Protocol*) e FTP (*File Transfer Protocol*);
- **Segurança**: pode executar programas via rede com restrições de execução;
- **Sintaxe**: similar a Linguagem C/C++;
- **Facilidades de Internacionalização**: suporta nativamente caracteres *Unicode*;
- **Simplicidade**: na especificação, tanto da linguagem como do "ambiente" de execução (JVM);
- **Distribuída**: com um vasto conjunto de bibliotecas (ou APIs - *Application Programming Interface*) e facilidades para criação de programas distribuídos e multitarefas (múltiplas linhas de execução em um mesmo programa);
- **Desalocação de Memória Automática**: feita por processo de coletor de lixo (G*arbage Collector*);
- **Carga Dinâmica de Código**: programas em Java são formados por uma coleção de classes armazenadas independentemente e que podem ser carregadas no momento de utilização.

2.3.2 – Vantagens

As vantagens de se utilizar Java consistem em:

- A linguagem Java funciona em qualquer sistema operacional, em qualquer arquitetura, ao contrário dos seus principais concorrentes;
- Não está limitada somente ao ambiente Windows;
- Java é uma arquitetura aberta, extensível, com várias implementações, o que a torna independente do fornecedor;
- É uma linguagem descomprometida, aceita inclusive nos meios universitários como uma boa linguagem para a aprendizagem, o que facilita o recrutamento de técnicos.

2.3.3 – Java 2D

O conhecimento a respeito das tecnologias Java para as plataformas *Web*, corporativa e móvel são bem conhecidas, porém muitos não conhecem as APIs Java para aplicações de domínios mais específicos, como manipulação e processamento de imagens. Java oferece um conjunto de modernas APIs gráficas que dão suporte aos mais diversos tipos de necessidades, como Java 3D, *Java Media Framework* (JMF) e Java 2D.

A API Java 2D oferece suporte à criação e manipulação de gráficos, imagens, animações, transformações geométricas e impressão, entre muitas outras funcionalidades. As classes da API são construídas sobre o tradicional *Abstract Window Toolkit* (AWT), estendendo funcionalidades existentes e acrescentando muitas novas. Tais classes são incluídas com o Java *Runtime Environment* (JRE) e ficam no pacote *java.awt* e em alguns subpacotes, como *java.awt.image e java.awt.image.geom*.

A classe *java.awt.Graphics2D* é a principal do Java 2D e estende *java.awt.Graphics*, a classe usada para a renderização antes da chegada do Java 2D. Ela representa o contexto gráfico e gerencia toda a renderização. Uma vez obtida uma instância de *Graphics2D*, temos disponíveis métodos para desenho de formas básicas, imagens, textos e outras operações gráficas. Para manipular gráficos em Java não criamos diretamente um objeto *Graphics2D*, ele é criado pela própria JVM e passado para a aplicação como parâmetro do método *paint().*

A API Java 2D usa dois sistemas de coordenadas: o espaço de usuário (*User Space*), que é independente de dispositivo e utilizado em todas as operações com o contexto *Graphics2D* e o espaço de dispositivo (*Device Space*), que corresponde aos *pixels*, pontos etc. do dispositivo utilizado. As coordenadas são convertidas automaticamente de um espaço para outro pelo Java 2D, garantindo a portabilidade e deixando o desenvolvedor despreocupado com detalhes de renderização dos dispositivos. Assim, a implementação é a mesma para um monitor ou para uma impressora. Na figura 19 é possível observar que a origem, coordenadas *x = 0* e *y = 0,* é correspondente a parte superior esquerda do painel, sendo que as coordenadas do eixo *x* crescem para a direita e as coordenas do eixo *y* para baixo.

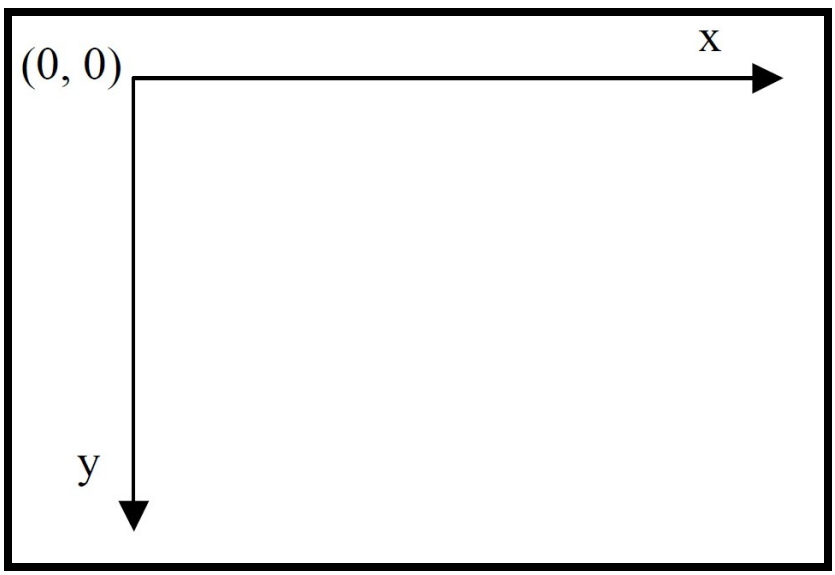

Figura 19 – Sistema de coordenas do Java 2D

O suporte à manipulação de gráficos e imagens oferecido por Java 2D é bastante rico. A API fornece recursos gráficos avançados para manipulações gráficas complexas e bastante detalhados. Sendo assim, a linguagem de programação escolhida para o desenvolvimento desse trabalho foi Java, devido á sua portabilidade e facilidade de utilização dos seus recursos de computação gráfica através do pacote Java2D.

2.4 – BANCO DE DADOS HSQLDB

O *Hypersonic SQL Database* (HSQLDB) é totalmente escrito em Java, distribuído livremente e pode ser utilizado em uma arquitetura cliente-servidor ou *standalone*. Sua utilização possibilita que o banco de dados seja agregado ao pacote de aplicações. Além disso, por ser escrito em Java, é multiplataforma e não ocupa muito espaço em disco. Com o HSQLDB é possível manipular bancos de dados em disco, memória ou em formato texto. Trata-se de uma tecnologia flexível e muito útil na construção de aplicações que manipulem banco de dados.

2.4.1 – Principais Características

As principais características apresentadas por HSQLDB são:

- Suporte à linguagem SQL (*Structured Query Language*) básica, incluindo junções, *triggers* e visões;
- Portabilidade em virtude de sua implementação ser feita em Java;
- Repositórios acessíveis através de tecnologia JDBC (*Java Database Connectivity*);
- Criação de bancos de dados em arquivo texto, banco de dados e em memória;
- Recurso de *dump* para *backups* facilitados;

- Ocupa pouco espaço em disco;
- Praticamente dispensa configurações para operar.

2.4.2 – Componentes do HSQLDB

No núcleo do pacote estão o RDBMS (*Relational Database Management System*) e o *driver* JDBC que disponibilizam as principais funcionalidades do banco, que são: o gerenciador de banco de dados relacional e o *driver* para conexão através de ligações Java. Além disso, o pacote contém um conjunto de componentes e ferramentas para execução do Sistema Gerenciador de Banco de Dados (SGBD). Através das ferramentas, podem se criar estruturas de um banco de dados, acessar bancos de dados através de ferramentas para consulta, exportar e importar esquemas entre bancos de dados distintos além de outras facilidades disponibilizadas para o desenvolvedor. De acordo com (SEVERO, 2008), as descrições de cada um desses componentes são:

- **HSQLDB JDBC Driver**: o pacote de distribuição disponibiliza um *driver* padrão JDBC para conexão de aplicações Java com o SGBD. A conexão com o banco de dados segue um modelo de protocolo proprietário, mas também pode realizar uma conexão via rede, através de protocolos *Internet*;
- **Database Manager**: duas versões de ferramentas para gerenciamento de banco de dados são disponibilizadas. Uma ferramenta escrita usando AWT e outra versão usando *Swing*. Trata-se de uma ferramenta gráfica para visualização do esquema do banco de dados, conjunto de tabelas e submissão de instruções SQL. A versão AWT pode ser executada como um *Applet* dentro de um navegador;
- **Transfer Tool**: é uma ferramenta utilizada para transferências de esquemas SQL ou dados de uma fonte JDBC para outra. Trata-se de uma ferramenta

bastante útil quando pretende realizar uma migração de banco de dados, transferindo esquemas e o conjunto de dados entre duas tecnologias distintas;

- **Query Tool**: a finalidade dessa ferramenta é prover ao desenvolvedor um *software* para interação com o SGBD através do envio de instruções SQL a partir de uma linha de comando, ou através de um arquivo texto contendo um conjunto de instruções. A ferramenta apresenta um *shell* interativo ao usuário;
- **SQL Tool**: outra ferramenta do pacote para construção e submissão de instruções SQL ao banco de dados.

Por ser escrito em Java e totalmente compatível com a linguagem, além de ser fácil de configurar e apresentar um ótimo desempenho foi o banco de dados escolhido para ser utilizado nesse projeto.

3 - SISTEMAS BIOMÉTRICOS

Neste capítulo serão feitas as fundamentações teóricas sobre sistemas biométricos. Serão apresentadas também as principais características biométricas, em especial a impressão digital.

3.1 – BIOMETRIA

O termo “Biometria” é utilizado para designar o estudo estatístico das características físicas ou comportamentais dos seres vivos, a fim de que estes possam ser manuseados (GREGORY; SIMNO, 2008).

Na área de segurança, refere-se ao conjunto de métodos automatizados para identificação de pessoas com base em suas características físicas ou aspectos comportamentais a fim de identificá-las unicamente (DESSIMOZ; RICHIARDI, 2006). Como a identificação é feita a partir de singularidades pertencentes às características biológicas ou comportamentais, esta técnica apresenta a vantagem de identificar o indivíduo sem a necessidade que esse possua objetos ou memorize algo (PACHECO, 2003).

A biometria tem a capacidade de distinguir de forma confiável um indivíduo autorizado de um impostor. Uma vez que as características biométricas são distintas, não podem ser esquecidas ou perdidas e o indivíduo a ser identificado necessariamente deve estar fisicamente presente no momento da identificação, a biometria torna-se mais segura do que as técnicas tradicionais de identificação ainda muito utilizadas (PRABHAKAR, 2001).

Os sistemas biométricos podem ser representados como um sistema de reconhecimento de padrões e são compostos basicamente pelo registro dos usuários e pelo posterior reconhecimento (DESSIMOZ; RICHIARDI, 2006). O

registro ocorre através da aquisição de dados biométricos de onde é extraído o perfil biométrico a ser armazenado na base de dados. O processo de comparação obtém os dados biométricos apresentados no momento da utilização e as características particulares dos dados são extraídas e comparadas com o perfil armazenado. Com base em um valor limite, o sistema decide se os dados apresentados são suficientemente similares ao perfil registrado (COSTA; OBELHEIRO; FRAGA, 2006). A figura 20 representa um sistema biométrico típico.

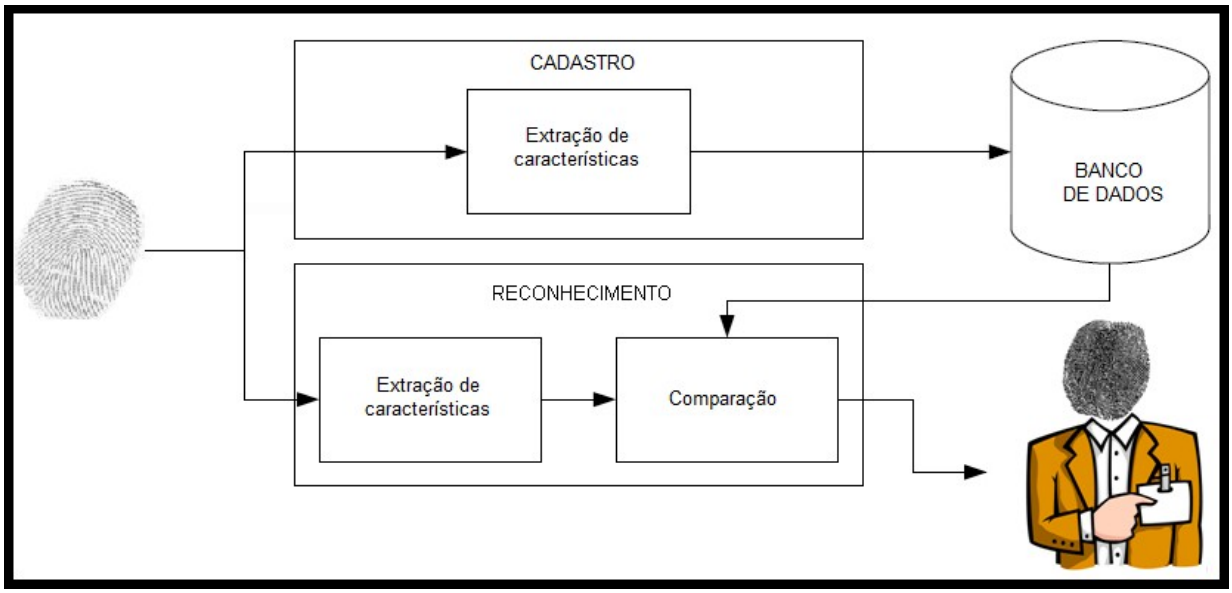

Figura 20 – Sistema biométrico típico

Os sistemas biométricos podem realizar o reconhecimento automático pessoal por duas formas distintas: autenticação e identificação. A autenticação está relacionada ao problema de confirmar ou negar a identidade de uma pessoa, que ao utilizar o sistema se identifica e apresenta sua característica biométrica. O processo de identificação é mais complexo, pois estabelece ou não a identidade de uma pessoa que no instante do reconhecimento apenas fornece seus dados biométricos (JAIN; BOLLE; PANKANTI, 2002).

3.1.1 – Vantagens dos Sistemas Biométricos

Os sistemas convencionais de identificação levam em consideração mecanismos que utilizam dois elementos: o que se sabe e o que se possui. O elemento conhecimento é o mais utilizado para fornecer uma identidade aos sistemas computacionais, como senhas, chaves de criptografia ou PIN (*Personal Identification Number*). As soluções baseadas na entidade propriedade caracterizam-se por um objeto físico que o usuário possui como cartões inteligentes (*smartcard*), cartões magnéticos ou *token*. A figura 21 ilustra a evolução dos dispositivos utilizados em sistemas de identificação.

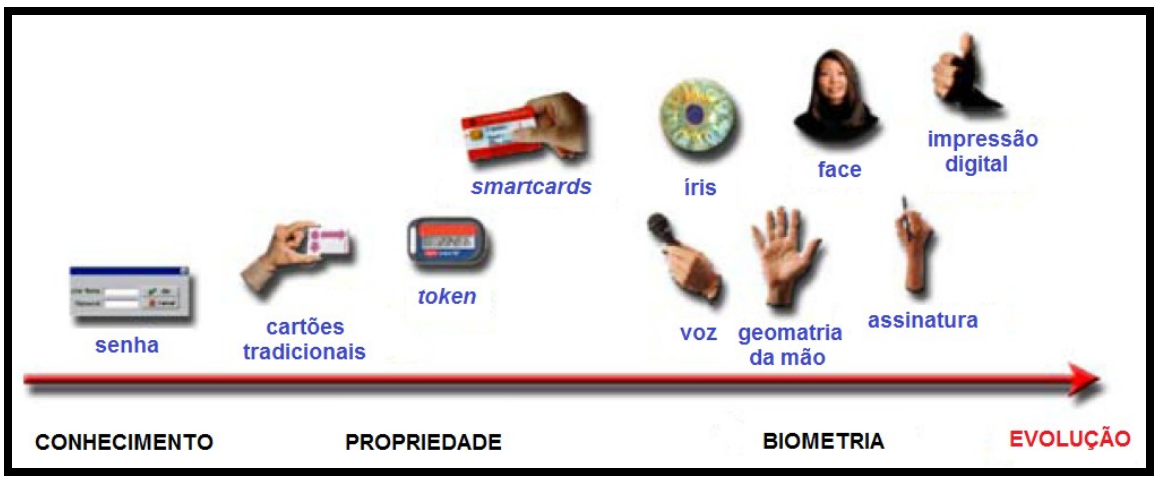

Figura 21 – Evolução dos dispositivos utilizados na identificação (COSTA, 2001)

Normalmente alguns sistemas usam a combinação de algo conhecido com a posse de objetos para identificação, o problema é que os objetos podem ser perdidos, roubados ou esquecidos e os códigos e senhas podem ser descobertos ou compartilhados. Uma vez que isso aconteça, qualquer pessoa não autorizada poderia se passar pelo legitimo usuário (JAIN; BOLLE; PANKANTI, 2002).

As três principais vantagens que o uso da biometria em lugar dos sistemas convencionais proporciona são:

- **Identificação mais confiável**: com a biometria, é mais provável que a pessoa que tenta obter acesso a determinado bem ou serviço é quem diz ser, uma vez que o risco de ter a chave biométrica perdida é bastante reduzido. É praticamente impossível que um impostor encontre um dedo ou olho perdido para se submeter ao reconhecimento biométrico;
- **Eliminação de compartilhamento de senha**: a característica biométrica está associada a uma única pessoa e não pode ser separada desta pessoa, o que elimina o compartilhamento de senhas por parte dos usuários;
- **Identificação mais conveniente**: a forma em que as soluções biométricas são implementadas podem tornar a identificação mais conveniente do que os sistemas convencionais. Apresentar a impressão digital para efetuar uma identificação é mais prático e leva menos tempo do que digitar o nome de usuário e a senha.

O uso de sistemas biométrico, além de proporcionar comodidade às pessoas pelo fato de não precisarem lembrar diversas senhas ou carregarem diversos cartões, também traz melhorias na segurança.

3.1.2 – Falsa Aceitação e Falsa Rejeição

O desempenho de um sistema biométrico pode ser obtido por meio da taxa de reconhecimento, levando-se em conta duas medidas: a taxa de falsa aceitação (FAR - *False Acceptance Rate*) e taxa de falsa rejeição (FRR - *False Rejection Rate*) (PEREIRA, 2003). A FAR é a probabilidade que tem um sistema biométrico de identificar incorretamente um indivíduo ou falhar na rejeição de um impostor, ou seja, representa a percentagem de usuários não autorizados que são incorretamente identificados como usuários válidos. Já a FRR é a probabilidade que tem um sistema biométrico de falhar na identificação de um usuário legítimo e representa a

percentagem de usuários cadastrados que são incorretamente rejeitados pelo sistema.

A taxa de erro igual (EER – *Equal Error Rate*) é o ponto em que a taxa de falsa aceitação é igual à taxa de falsa rejeição. Dessa forma, um sistema que apresente tanto a FRR como a FAR de 1%, também terá um EER de 1%. Este é um parâmetro muito importante na avaliação de algoritmos de reconhecimento, de forma que quanto menor a EER, melhor o algoritmo.

A figura 22 mostra um gráfico onde é possível observar a relação existente entre as taxas FAR, FRR e EER.

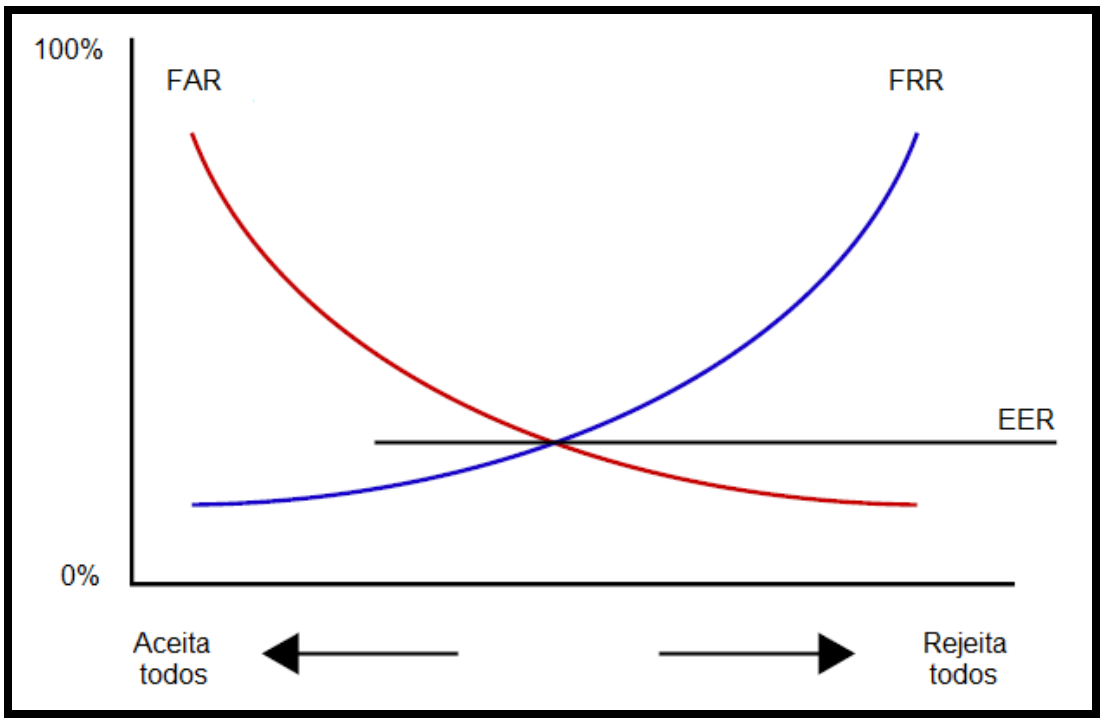

Figura 22 – Relação entre FAR, FRR e ERR (PEREIRA, 2003)

O nível de precisão configurado no algoritmo de comparação tem efeito direto nessas taxas. O modo como estas são determinadas é fundamental para a operação de qualquer sistema biométrico e assim deve ser considerado um fator primário na avaliação de sistemas biométricos (PEREIRA, 2003). Um sistema geralmente pode

ser ajustado para taxas de FAR e FRR adequadas, porém diminuindo uma aumenta a outra e vice-versa. A falsa rejeição causa frustração nos usuários e a falsa aceitação possibilita fraudes. Por isso a configuração do valor limite para tolerância a estes erros é crítica no desempenho do sistema.

3.1.3 – Autenticação e Identificação

Um ponto importante da biometria é a diferença entre autenticação e identificação. Na autenticação, uma pessoa precisa informar ao sistema sua identidade juntamente como o dado biométrico. O sistema apenas diz se a pessoa é quem diz ser ou não. Esse processo é conhecido como comparação 1:1, pois a pessoa informa ao sistema qual perfil deve ser comparado com a amostra fornecida no momento do reconhecimento. A figura 23 ilustra o processo de autenticação.

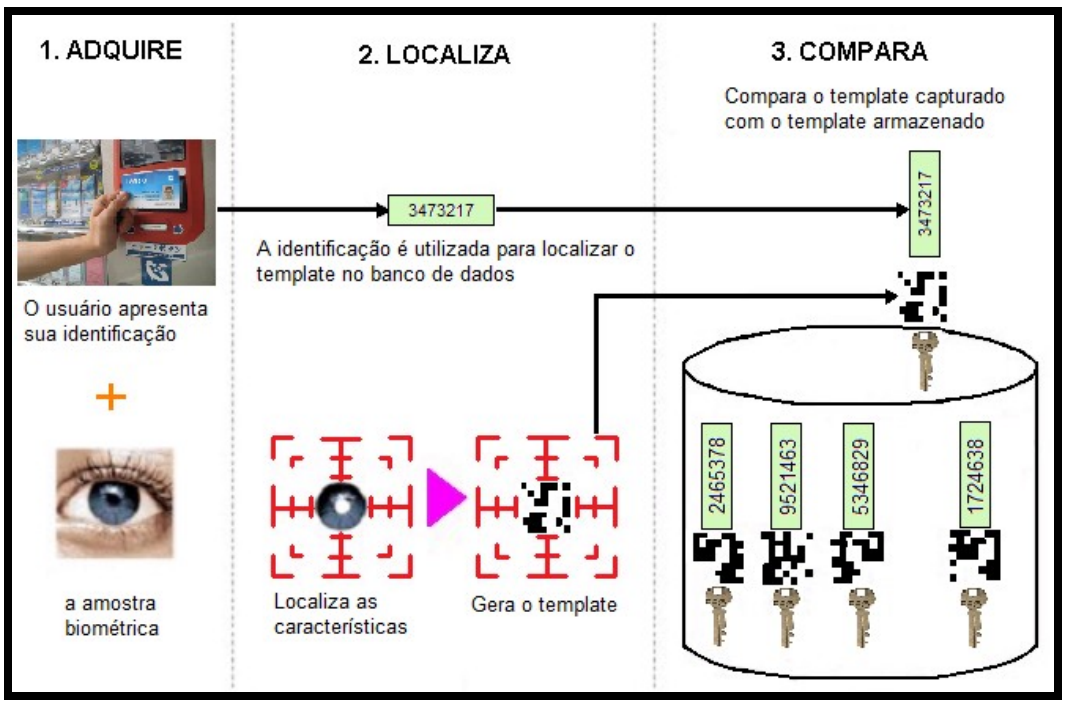

Figura 23 – Sistema biométrico de autenticação (PEREIRA, 2003)

Na identificação apenas com a leitura biométrica o sistema é capaz de dizer quem é a pessoa. É um processo conhecido como comparação 1:N, uma vez que o sistema pega a amostra biométrica e compara com todos os perfis armazenados no banco de dados, informando, caso exista um perfil com a semelhança exigida, quem é a pessoa. A figura 24 mostra o processo de identificação.

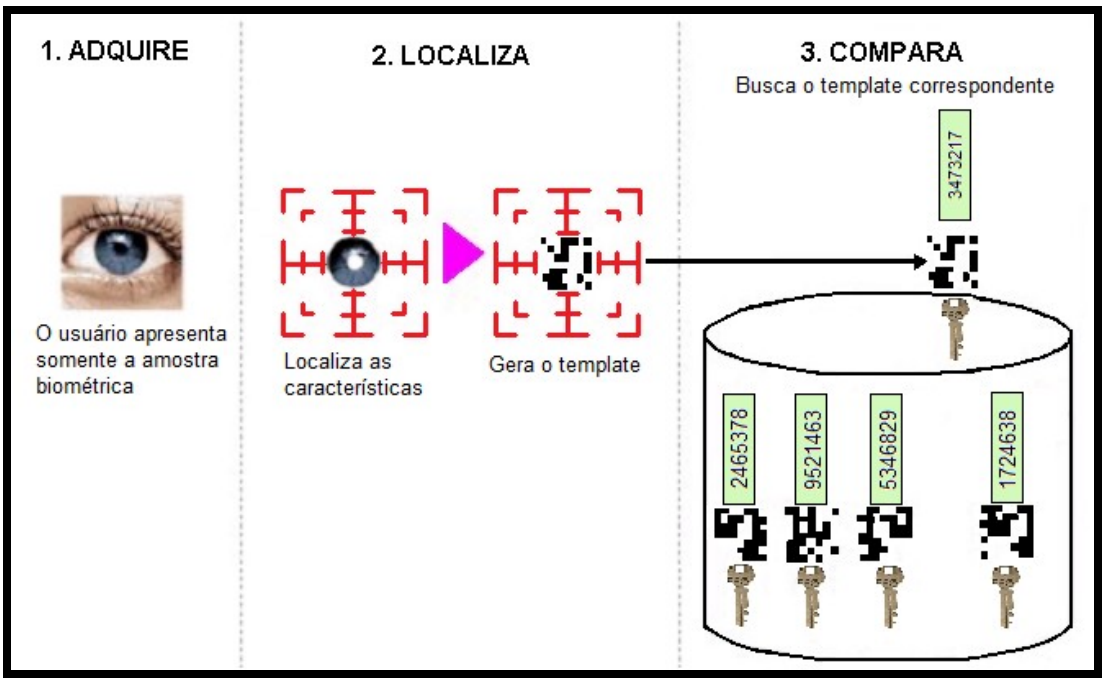

Figura 24 – Sistema biométrico de identificação (PEREIRA, 2003)

Apenas uma comparação é realizada na autenticação, o que facilita muito sua implementação, mas exige algum componente extra de identificação, como um código pessoal. A identificação é muito utilizada pela polícia que pode identificar um criminoso, mesmo que não exista uma lista de suspeitos, apenas pela obtenção das impressões digitais por ele deixadas na cena do crime.

Existem dois modos possíveis para identificação: positivas e negativas. A identificação positiva procura determinar se uma pessoa realmente está cadastrada em uma base de dados específica, sendo aplicada quando o objetivo é verificar uma identidade única entre várias outras. Contrariamente, a identificação negativa determina se o cadastro de uma pessoa não está presente em um banco de dados,

podendo ser utilizada para verificar se a referida identidade não consta em uma lista de procurados (DESSIMOZ; RICHIARDI, 2006).

3.1.4 – Características Biométricas

Qualquer característica física ou comportamental do ser humano pode ser usada na identificação biométrica, desde que apresente as seguintes propriedades: universalidade, que significa que a característica deve ser comum a todas as pessoas; unicidade, que garante que a característica seja única para cada indivíduo; permanência, pois a característica não pode sofrer grandes alterações com o passar do tempo; coleta, que indica que a característica pode ser medida quantitativamente. Além disso, a característica deve ter a aceitação pública e ser de fácil aquisição (MAZI, 2009).

A biometria pode utilizar aspectos comportamentais ou características físicas do usuário. Dados como os da impressão digital, face, íris e formato da mão são classificadas como características físicas ou estáticas. Já o reconhecimento de voz e a análise de assinatura encontram-se no grupo de características comportamentais ou dinâmicas (GARCIA et al., 2003). A tabela 2 mostra um comparativo entre as principais características biométricas.

Biometria	Universalidade	Unicidade	Permanência	Coleta	Aceitação
Digital	Média	Alta	Alta	Média	Média
Face	Alta	Baixa	Média	Alta	Alta
Íris	Alta	Alta	Alta	Média	Baixa
Mão	Média	Média	Média	Alta	Média
Assinatura	Baixa	Baixa	Baixa	Alta	Alta
Voz	Média	Baixa	Baixa	Média	Alta

Tabela 2 – Comparativo entre características biométricas (COSTA, 2007)

Visto que há diversas características biométricas que podem ser utilizadas em processos de identificação, é necessário verificar qual o objetivo da aplicação e como a característica será utilizada para então escolher qual se encaixa melhor. Desta forma, a aplicação faz uso dos recursos biométricos e consegue obter as reais vantagens deste uso (ALVES, 2007). Outro ponto a considerar é o tamanho do modelo biométrico que será armazenado, que pode variar de acordo com a característica escolhida. A tabela 3 mostra em *bytes* o tamanho dos modelos biométricos.

Biometria	**Tamanho em *bytes***
Digital	256 - 1200
Face	84 - 2000
Íris	96
Mão	9
Assinatura	500 - 1000
Voz	70 - 80

Tabela 3 – Tamanho aproximado do modelo biométrico (JUNIOR; ORLANS; HIGGINS, 2002)

O uso de características biométricas para identificação é viável porque se apresentam de formas diferentes em cada pessoa, nem mesmo entre irmãos gêmeos, que apesar de serem muito parecidas, elas não são idênticas.

3.1.5 – Tecnologias Biométricas

Dentre as diversas características biométricas que podem ser utilizadas em sistemas biométricos, as mais comuns são impressão digital, aparência da face, padrão da íris, geometria da mão, dinâmica da assinatura e padrão da voz (COSTA, 2007). Além destas, existem sistemas biométricos que se baseiam na arquitetura da orelha, análise de retina, arcada dentária, palma da mão, dinâmica de digitação, na forma

de andar, padrão vascular, termograma facial, odor, movimento labial, DNA (*Deoxyribonucleic Acid*, ou em português, Ácido Desoxirribonucléico) e até em ondas cerebrais (GREGORY; SIMNO, 2008). A figura 25 mostra as características biométricas mais comuns.

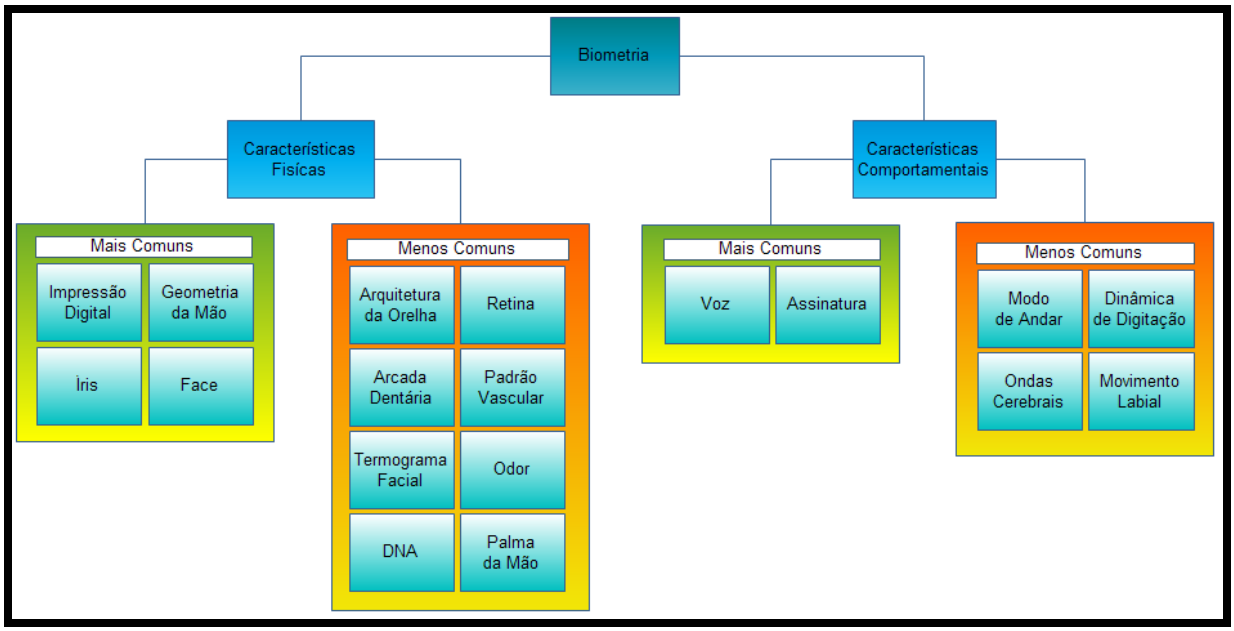

Figura 25 – Características biométricas mais comuns e outras (COSTA; OBELHEIRO; FRAGA, 2006)

3.1.5.1 – Impressão Digital

A Impressão digital é formada durante a gestação, sendo constituída por sulcos presentes nas pontas dos dedos. A forma como estes sulcos estão dispostos formam as características da impressão digital, as minúcias, que são únicas em cada indivíduo. Estas características são extraídas através de um software de processamento de imagem e transformadas em um modelo biométrico que é utilizado para o reconhecimento. A impressão digital é o método mais utilizado, pois além de ser mais barato também é muito seguro. A figura 26 mostra o dispositivo de reconhecimento por impressão digital.

Figura 26 – Reconhecimento por impressão digital (HOUSE, 2010)

3.1.5.2 – Face

Entre os seres humanos, o reconhecimento facial é o método mais utilizado para reconhecer pessoas. Através da expressão facial é possível também perceber facilmente o estado emocional de um indivíduo.

O processo automatizado utiliza uma imagem obtida através de um *scanner* ou câmera digital que depois é analisada, por meio de vários tipos de algoritmos que utilizam pontos delimitadores na face para definir distâncias, tamanhos e formas de cada elemento do rosto como olhos, nariz, queixo e orelhas com o objetivo de se obter um padrão biométrico.

Embora o reconhecimento facial seja uma tarefa rotineira para os humanos, para uma máquina é extremamente complexa a tarefa de comparar duas imagens digitais de face. O problema é que a máquina não tem a capacidade que os humanos têm

de observar as alterações típicas da aparência facial como expressões, presença de barba, maquiagem ou mudanças no corte de cabelo (GREGORY; SIMNO, 2008).

A figura 27 mostra o reconhecimento através da face.

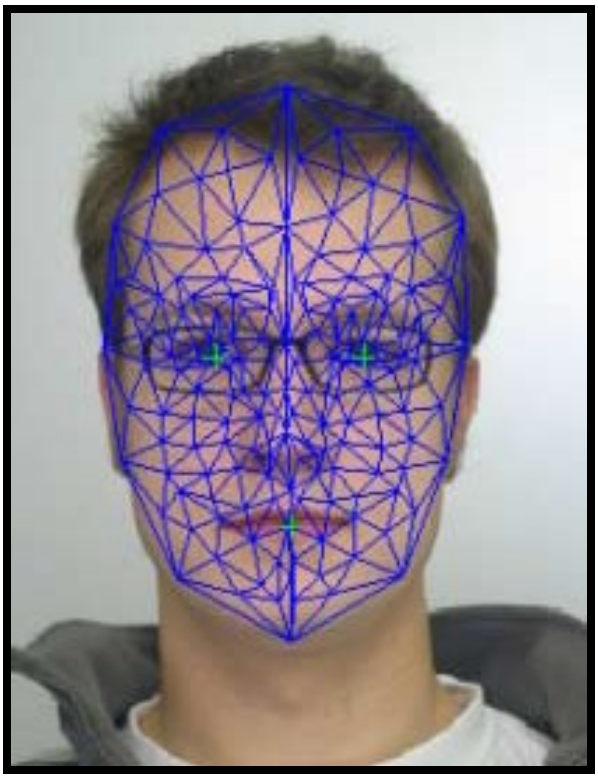

Figura 27 – Reconhecimento facial (KENTUCKY, 2010)

3.1.5.3 – Íris

A íris é a parte do olho formada por anéis coloridos existente em torno da pupila, por isso prende mais a atenção, sendo muito utilizada pelas pessoas quando querem lembrar ou caracterizar alguém. A estrutura da Íris é complexa e única em cada pessoa, o que a torna uma característica para identificação biométrica. Uma imagem digital da íris tirada sob uma iluminação infravermelha é processada por algoritmos que extraem a amostra biométrica necessária para o processo de reconhecimento (GREGORY; SIMNO, 2008). A figura 28 mostra o reconhecimento pela íris.

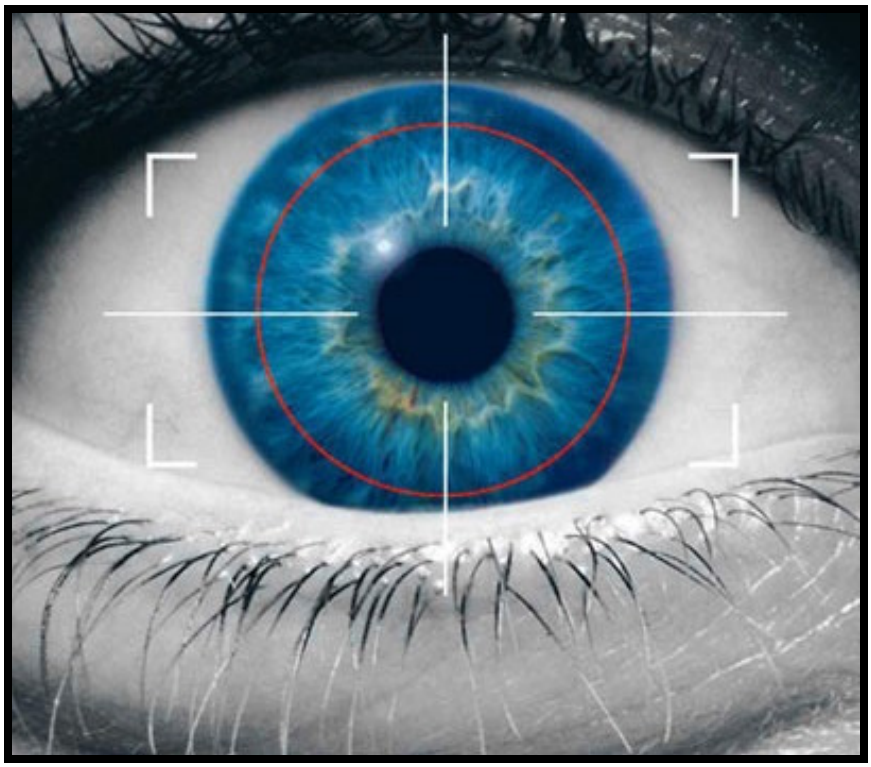

Figura 28 – Reconhecimento por íris (DETROIT, 2010)

3.1.5.4 **–** Geometria da Mão

A geometria da mão é outro método que também pode ser usado no processo de reconhecimento. Consiste na medição da mão, tamanho do dedo, largura e área. Estas características são distintas o suficiente para permitir a autenticação de um indivíduo, no entanto, não são suficientes para uma pesquisa de identificação (JUNIOR; ORLANS; HIGGINS, 2002). No momento da utilização o usuário posiciona sua mão no leitor, sempre na mesma posição, e uma câmera posicionada acima captura a imagem. Para que não ocorra a rotação da mão durante a utilização, os dispositivos leitores contêm pinos que indicam onde cada dedo deve ficar posicionado, melhorando a qualidade da imagem (PEREIRA, 2003). A figura 29 mostra o reconhecimento através da geometria das mãos.

Figura 29 – Reconhecimento pela geometria da mão (OREGON, 2010)

3.1.5.5 – Assinatura

A assinatura pode ser usada em um sistema de identificação biométrica de dois métodos: um examina a assinatura já escrita, como se fosse uma imagem, e compara com o modelo armazenado; o outro não se baseia apenas na comparação de assinaturas, mas consiste em analisar características tais como velocidade, direção e pressão exercida durante o processo de realizar a assinatura. Os dispositivos utilizados para análise dinâmica são canetas óticas e superfícies sensíveis (COSTA; OBELHEIRO; FRAGA, 2006). A figura 30 mostra o reconhecimento por assinatura.

Figura 30 – Reconhecimento de assinatura (ZONE, 2010)

3.1.5.6 – Voz

O reconhecimento de voz analisa o som produzido pelas cordas vocais e é um dos sistemas menos invasivos. O reconhecimento leva em consideração características como a frequência e o tamanho das ondas sonoras que estão relacionadas ao formato da boca e cavidades nasais. Durante o processo de captura o usuário utiliza um microfone para pronunciar algo específico ou uma frase qualquer, repetida vezes, para a extração de um modelo biométrico (PEREIRA, 2003). A figura 31 mostra como é o reconhecimento de voz.

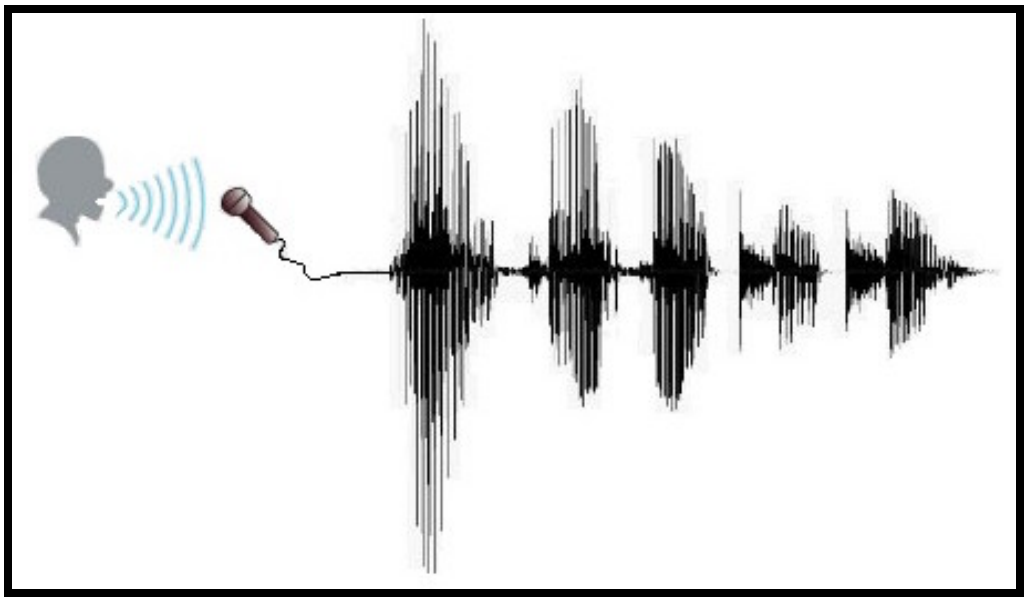

Figura 31 – Reconhecimento de voz

Dentre as características biométricas existentes algumas são mais utilizadas devido ao melhor custo/beneficio e também pela facilidade de utilização devido a vários aplicativos no mercado. A tabela 4 mostra em porcentagem a utilização das principais características biométricas.

Tecnologia	Utilização
Digital	52%
Face	16%
Íris	12%
Voz	10%
Mão	6%
Assinatura	3%

Tabela 4 – Utilização das principais características biométricas (COSTA, 2007)

Considerando as características biométricas apresentadas, a impressão digital e a íris são as que menos sofrem alterações com o tempo. A íris pode fornecer a maior precisão, embora a impressão digital seja a mais utilizada (COSTA, 2007).

3.1.6 – Aplicações da Biometria

As tecnologias biométricas podem ser utilizadas para aumentar a segurança e a agilidade nas operações de uma ampla variedade de aplicações, que vão desde sistemas de segurança até aplicações para controle de frequência (COSTA, 2007). Estas tecnologias podem ser aplicadas em diversas áreas: controle de acesso, identificação civil, identificação criminal, comércio eletrônico, etc. Algumas dessas aplicações serão abordadas com mais detalhes.

3.1.6.1 - Controle de Acesso

A biometria pode ser utilizada para restringir o acesso a um local ou área restrita. O acesso pode ser tanto físico como lógico. O acesso físico ocorre quando o indivíduo tenta acessar um edifício, um prédio, uma garagem ou sala, por exemplo. Já o acesso lógico ou virtual é feito por meio de um sistema computadorizado, como o acesso a base de dados, aplicações ou a rede de computadores de uma organização. Ambientes que exigem alto nível de segurança, já há alguns anos, vêm utilizando a biometria para controle e acesso. A figura 32 mostra como é feito este controle de acesso: à esquerda utilizando biometria e a direita por meio de métodos convencionais.

Figura 32 – Controle de acesso (TECHNOLOGIES, 2010)

3.1.6.2 – Identificação Civil

Os órgãos de governos e repartições públicas utilizam a biometria para identificar ou verificar a identidade dos cidadãos. Isso engloba a emissão de documentos como carteira de identidade, passaporte, controle de imigração, carteira de habilitação, verificação de antecedentes e serviços de seguridade sociais. O Tribunal Superior Eleitoral (TSE) está testando urnas eletrônicas que utilizam sistema de identificação biométrica dos eleitores. O objetivo principal é diminuir a fraude no processo de eleição, evitando que uma pessoa vote no lugar de outra. A figura 33 mostra uma urna eletrônica que utiliza biometria para a identificação dos eleitores.

Figura 33 – Urna biométrica (TRE/RO, 2010)

3.1.6.3 – Identificação Criminal

Por anos a biometria tem sido utilizada para identificar suspeitos ou indivíduo em questões legais ou de combate ao crime. Este tipo de aplicação biométrica foi a primeira a ser largamente difundida, utilizando dados da impressão digital para o reconhecimento pessoal. A figura 34 mostra a coleta de impressão digital em um automóvel.

Figura 34 – Coleta de impressão digital (HEALTH HAVEN, 2010)

3.1.6.4 – Comércio Eletrônico

O número de fraudes nesse setor apresenta um acréscimo considerável a cada dia, sendo necessário o uso de mecanismos mais eficazes para a identificação dos usuários. Dessa forma, a biometria pode ser utilizada para identificar indivíduos em transações remotas, visando produtos ou serviços como aplicações bancárias e aplicações na *Web*, oferecendo muito mais segurança aos seus usuários e ao mesmo tempo reduzindo os prejuízos com fraudes.

3.1.6.5 – Pontos de Vendas

A garantia de que o indivíduo esteja fisicamente presente no momento da transação pode ser conseguida com o uso da biometria, que neste caso, identifica o consumidor que está conduzindo a transação em pessoa. Neste contexto, quando uma tecnologia biométrica é utilizada, dificilmente uma pessoa conseguirá se passar por outra.

3.1.6.6 – Vigilância

Outro uso da biometria é a vigilância para identificar os indivíduos presentes ou em movimento em determinas áreas. Tipicamente, bancos ou aeroportos fazem a vigilância com câmeras que pode ser complementada com a biometria para determinar a identidade das pessoas que circulam por estas áreas. A figura 35 mostra alguns locais onde tem câmeras de vigilâncias instaladas.

Figura 35 – Câmeras de vigilância (DIREITA, 2010)

A biometria tem sido amplamente utilizada em aplicações para a identificação criminal e por isso está evoluindo rapidamente, e tem um potencial de crescimento para ser amplamente adotada em aplicações civis tais como *Internet Bank*, *e-commerce* e controle de acesso. A utilização destas operações cresce de forma rápida tornando-se uma das mais importantes aplicações de biometria. A tabela 5 mostra a distribuição por finalidade das aplicações biométricas.

Finalidade	Utilização
Identificação Criminal	28%
Controle de Acesso	22%
Identificação Civil	21%
Pontos de Venda	4%
Comércio Eletrônico	3%
Vigilância	3%

Tabela 5 – Distribuição por finalidade (COSTA, 2007)

Com o avanço da tecnologia biométrica, aplicações que envolvem cartões de crédito, *smartcards*, caixas eletrônicos, operações *on-line* e até o controle de acesso, antes baseadas em processos de reconhecimento tradicional, passarão a utilizar cada vez mais a biometria que, com o tempo, amadurece e torna-se digna de confiança (PRABHAKAR, 2001).

3.2 – IMPRESSÃO DIGITAL

Será feita uma análise mais detalhada da impressão digital, tendo em vista que o sistema biométrico que foi desenvolvido neste projeto envolve este tipo de característica.

A impressão digital é formada por sulcos presentes nas pontas de cada um dos dedos. A parte alta dos sulcos é denominada de crista e a baixa denominada de vale. A formação das impressões digitais é bem conhecida e têm sido amplamente utilizadas, desde o início do século XX, para identificação de criminosos pelos diversos serviços forenses em todo o mundo (PRABHAKAR, 2001).

Como a primeira utilização das impressões digitais para a identificação está relacionada à área penal, algumas pessoas se sentem desconfortáveis em fornecer suas impressões em aplicações civis. Entretanto, por oferecer um elevado grau de confiança, os sistemas biométricos de identificação baseados em impressões digitais estão se tornando cada vez mais populares (PRABHAKAR, 2001).

A impressão digital pode ser utilizada para a identificação pessoal de duas formas: manual e automática. A análise manual é realizada pela visualização, com o auxílio de lentes de aumento, das características das impressões digitais e pela comparação entre elas, determinando se são iguais ou não. Este modo de análise pode levar dias dependendo do tamanho do banco de dados, pois este processo é realizado com cada uma das impressões digitais armazenadas, até que se obtenha ou não a identificação. A figura 36 mostra um individuo analisando manualmente uma impressão digital.

Figura 36 – Análise manual de impressões digitais (G1.com, 2010)

Este problema pode ser contornado pela automatização do processo, por meio da utilização de *hardware* e *software* específicos para processamento digital da imagem, que além de diminuir o tempo de resposta, não prende o ser humano a tediosa tarefa de analisar e comparar as impressões digitais (COSTA, 2001).

A impressão digital é única em cada indivíduo e, exceto pelo aumento de tamanho durante a fase de crescimento ou quando ocorre algum ferimento ou corte muito profundo, não sofre alterações durante a vida toda. Isso faz com que a impressão digital seja uma das características mais utilizadas nos processos de identificação biométrica.

3.2.1 – Formação e Constituição

O conjunto de cristas e vales que constituem a impressão digital forma desenhos característicos. Estes desenhos são desenvolvidos durante os primeiros sete meses de gestação do feto, como consequência genética e também pelas condições do ambiente uterino, e a configuração dos seus traços não sofre alterações durante a vida toda (PRABHAKAR, 2001).

A posição no interior do útero e o fluxo de líquidos em torno do feto mudam durante a gestação fazendo com que as células dos dedos cresçam em um microambiente diferente. Os dedos de cada indivíduo e os próprios dedos de uma mesma pessoa apresentam detalhes que são determinados pelas mudanças dos diferentes microambientes onde estão inseridos.

Devido ao grande número de mudanças que ocorre durante o processo de gestação, é praticamente impossível que duas impressões digitais sejam iguais, embora, pelo fato dos genes também contribuem para sua formação, alguns dos traços que definem a impressão digital podem apresentar grandes semelhanças, principalmente entre gêmeos idênticos (PRABHAKAR, 2001). A figura 37 mostra as impressões digitais de gêmeos idênticos.

Figura 37 – Impressões digitais de gêmeos idênticos (PRABHAKAR, 2001)

Entre pai e filho esta semelhança também existe, por compartilharem metade dos genes. Pessoas da mesma raça e sem grau de parentesco possuem similaridade muito pequena nas digitais, enquanto que os indivíduos de raças diferentes apresentam a máxima diferença entre elas (COSTA; OBELHEIRO; FRAGA, 2006).

3.2.2 – Classificação

As impressões digitais podem ser divididas em várias classes de acordo com sua topologia geométrica. Edward Henry foi o primeiro a propor um sistema de classificação de impressões digitais, o *Henry System* que classifica as impressões digitais em cinco classes (COSTA, 2001). Estas classes são baseadas em dois tipos de pontos singulares: núcleos e deltas. O núcleo é um ponto localizado na área central da impressão digital sendo a volta mais interna do conjunto das cristas. O delta é um triângulo formado pelas cristas e corresponde ao maior ângulo entre elas. A figura 38 mostra o núcleo e deltas em uma impressão digital.

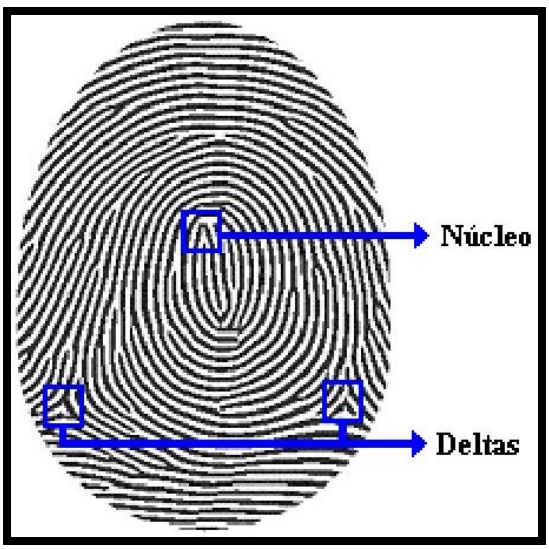

Figura 38 – Núcleo e deltas em impressão digital (MAZI, 2009)

As linhas das impressões digitais são classificadas em cinco classes:

- **Arco Plano**: as linhas que formam a impressão digital atravessam de um lado para outro de forma abaulada. Não apresentam delta;
- **Arco Angular**: apresentam acentuada elevação das linhas no centro, em forma de tenda. Pode apresentar um delta, mas sem linha entre o delta e o núcleo;

- **Presilha Interna (Direita)**: as linhas formam-se à esquerda do observador, curvam- se no centro e tendem a voltar ao mesmo lado, com um delta à direita do observador;
- **Presilha Externa (Esquerda)**: as linhas formam-se à direita do observador, curvam-se no centro e tendem a voltar para o mesmo lado, com um delta à esquerda do observador;
- **Verticilo**: apresentam dois deltas, sendo um à direita e outro à esquerda do observador. As linhas nucleares tendem a ficar entre os dois deltas, apresentando um padrão concêntrico, espiralado, oval ou sinuoso no centro da impressão digital.

A figura 39 mostra a classificação das linhas das impressões digitais.

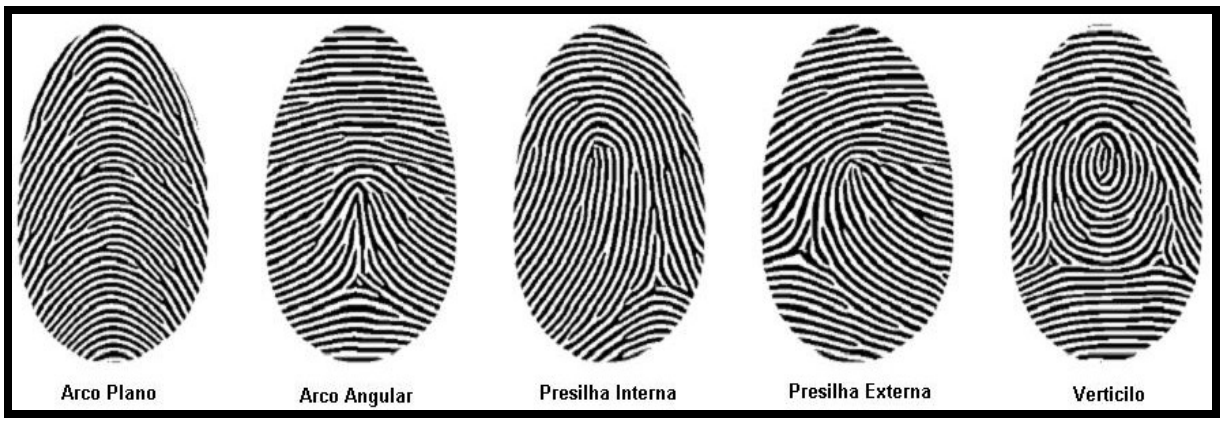

Figura 39 – As cinco classes do *Henry System* (MAZI, 2009)

A distribuição das impressões digitais na população não ocorre de forma uniforme entre as cinco classes. Das impressões digitais arquivadas pelo FBI (*Federal Bureau of Investigation*), 65% são classificadas como presilhas, 30% são verticilos e 5% arcos (COSTA, 2001).

Os pontos singulares, delta e núcleo, são usados para efetuar a classificação da impressão digital. A separação das impressões digitais em classes é normalmente

utilizada para a indexação, reduzindo o tempo de processamento durante a identificação, uma vez que é necessário apenas efetuar comparações com as impressões da mesma classe (DESSIMOZ; RICHIARDI, 2006).

3.2.3 – Minúcias

A forma como os sulcos da impressão digital estão dispostos formam as características da impressão digital. Tais características, chamadas de pontos de minúcias, apresentam diferenças que podem ser medidas e utilizadas no processo de identificação. Essas pequenas irregularidades, que ocorrem nas cristas das impressões digitais estabelecem a distinção entre elas e garante a unicidade, sendo necessárias doze minúcias para se obter, com certo grau de certeza, a identidade de uma pessoa (COSTA, 2001).

Uma imagem de impressão digital com boa qualidade normalmente contém entre 60 e 80 minúcias (PRABHAKAR, 2001). Existem vários tipos de classificação de minúcias, porém os mais utilizados para o reconhecimento de impressões digitais são as minúcias do tipo terminais e as minúcias do tipo bifurcadas. A figura 40 mostra a classificação das minúcias.

Figura 40 – Classificação de minúcias (FARIA, 2005)

Os sistemas de reconhecimento automático de impressão digital utilizam apenas dois tipos de minúcias, terminais e bifurcadas. O FBI também considera somente terminações e bifurcações para a identificação de indivíduos. As bifurcações ocorrem quando uma crista da impressão digital se divide em duas outras e as terminações ocorrem quando uma crista se interrompe. A figura 41 mostra a minúcias utilizadas em sistemas biométricos automáticos.

Figura 41 – Minúcias utilizadas em sistemas biométricos (FARIA, 2005)

As minúcias são caracterizadas por três parâmetros: tipo, posição e orientação (PACHECO, 2003). O tipo da minúcia define se esta é uma terminação ou uma bifurcação, a posição indica o local ou coordenada (*x, y)* onde se verifica a existência da minúcia e a orientação é o ângulo entre a tangente à crista da minúcia e o eixo horizontal.

As minúcias também são chamadas de pontos característicos ou “Detalhes de Galton”, em referência a Francis Galton, que foi o primeiro a categorizar e observar que as minúcias não se modificam ao longo da vida (COSTA, 2001). A classificação das impressões digitais quanto à quantidade e localização de núcleos e delta são exemplos de características globais. Já as minúcias são usadas para obter uma caracterização única de uma determinada impressão digital.

3.2.4 – Aquisição de imagem

As imagens de impressões digitais podem ser adquiridas pela utilização de tinta e papel e posterior digitalização da imagem, método *off-line*, ou por meio de sensores apropriados, método *on-line* (PRABHAKAR, 2001). Existe ainda outra forma, a utilização de imagem sintética de impressões digitais.

3.2.4.1 – Método *Off-Line*

O primeiro processo é chamado de *inked* e pode ocorrer de três formas: *rolled*, *dab* e *latent*. Nas duas primeiras formas é aplicada uma camada de tinta na superfície do dedo que em seguida é aplicado sobre uma folha de papel, este papel é então digitalizado em tons de cinza. O que difere as duas formas é como o dedo é aplicado sobre o papel, sendo que na primeira o dedo é rolado de um lado para o outro enquanto que na segunda o dedo é apenas pressionado contra o papel. Já a forma *latent* é obtida por impressões digitais que os dedos deixam na superfície de objetos, devido à presença de suor e gordura. Este método é utilizado pela polícia que tipicamente recolhe as impressões digitais encontras em cenas de crimes. A figura 42 mostra o método *inked.*

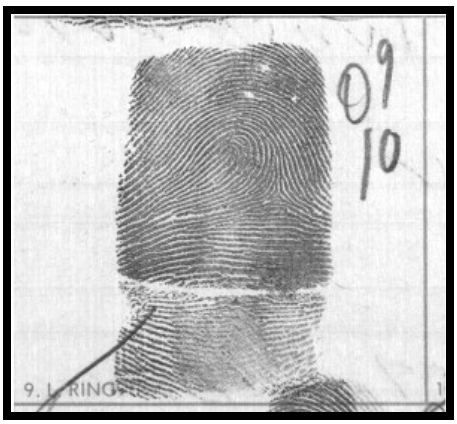

Figura 42 – Impressão digital adquirida utilizando o método *inked* (PRABHAKAR, 2001)

3.2.4.2 – Método *On-Line*

O segundo processo é chamado de *live-scan*, onde a imagem ao vivo é obtida diretamente do dedo por meio de um dispositivo eletrônico. A aquisição de imagens ao vivo está baseada em quatro principais tecnologias: ótica, capacitiva, térmica e ultra-sônica (COSTA, 2007). No sensor óptico, o dedo é colocado sobre uma plataforma de vidro e uma imagem do dedo refletida de um prisma é capturada. A tecnologia capacitiva utiliza as cargas elétricas, que são diferentes em função da distância entre as cristas e vales quando o dedo toca uma placa de silício, convertendo-as num valor de intensidade de um *pixel*. A tecnologia térmica funciona de forma semelhante à capacitiva, baseando-se no fato de que as cristas e os vales produzem temperaturas diferentes, o que causa alterações na temperatura da superfície do sensor. O sensor de ultra-som consiste de um sinal acústico enviado e dirigido através da superfície do dedo, o eco resultante ou sinal refletido é captado para medir diretamente a profundidade dos sulcos, funcionando como uma ultra-sonografia. A figura 43 mostra o método *live-scan.*

Figura 43 – Impressões digitais adquiridas utilizando o método *live-scan* (PRABHAKAR, 2001)

Na prática, as imagens adquiridas pelo método *off-line* podem apresentar borrões e manchas por excesso ou falta de tinta, afetando muito a qualidade da imagem que é

de extrema importância em um sistema de reconhecimento. Por isso, o método de aquisição *on-line* é mais eficiente, além de ser mais rápido e dispensar gastos com tinta e papel. Na figura 44 é possível observar a diferença de qualidade entre os métodos para uma mesma impressão digital.

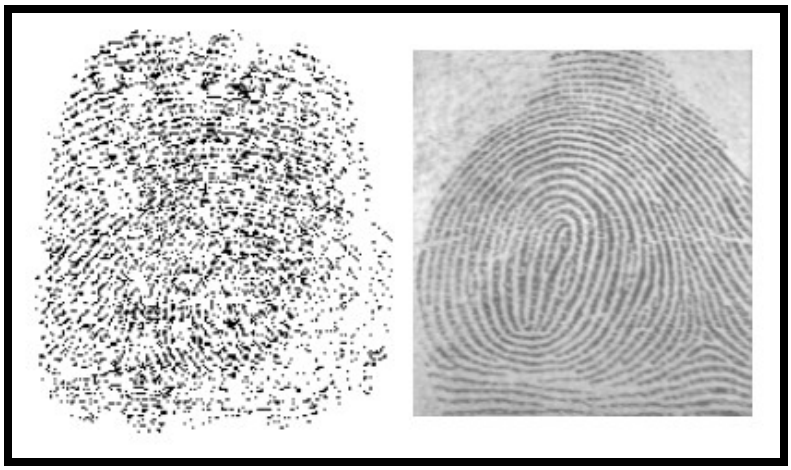

Figura 44 – Método *off-line* (esquerda) e método *on-line* (direita) (COSTA, 2001)

3.2.4.3 – Impressão Digital Sintética

Nas seções anteriores foram descritas maneiras de como capturar e gerar imagens reais de impressão digital através de duas formas: método *off-line* ou diretamente por um sensor, método *on-line*. Entretanto, coletar impressões digitais para formar um grande banco de dados não é uma tarefa fácil. Isso se deve a grande demanda de tempo e dinheiro necessários para a sua realização. Além disso, alguns países proíbem a divulgação de tais informações pessoais.

Para contornar esses problemas, muitas vezes as imagens de impressão digital utilizada pelos sistemas biométricos são geradas de forma sintética, obtidas por *softwares* capazes de gerar grandes bancos de dados de imagens a partir de modelos matemáticos que descrevem as principais características das impressões digitais reais.

As imagens de impressão digital sintética são geradas aleatoriamente de acordo com alguns parâmetros que garantem a unicidade entre elas, resultando em imagens muito realistas e semelhantes às impressões digitais humanas. Dessa forma os desenvolvedores podem testar suas aplicações, sem maiores problemas, com imagens sintéticas.

O *software SFinGe* (*Synthetic Fingerprint Generator*) desenvolvido pelo BioLab (*Biometric System Laboratory*) da Universidade de Bologna, na Itália, é um ótimo gerador de impressões digitais sintéticas. As bases de dados de impressão digital por ele geradas estão sendo amplamente utilizadas por organizações acadêmicas, industriais e governamentais para desenvolvimento, otimização e testes de seus sistemas biométricos (BIOLAB, 2010). A figura 45 mostra a interface inicial da versão demonstrativa do aplicativo *SFinGe*.

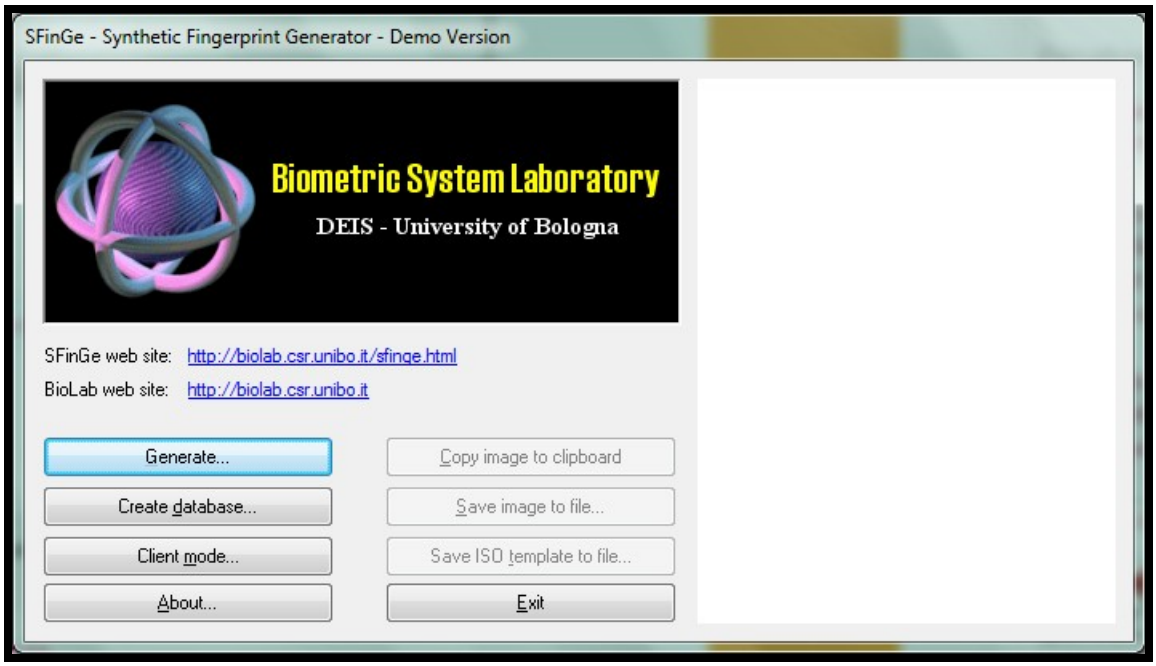

Figura 45 – Aplicativo *SFinGe*

A opção "*Create database*" do *SFinGe* só está disponivel na versão completa, que não é gratuíta. Mas o BioLab disponibiliza uma versão demonstrativa que oferece

muitas opções no processo de geração de impressões digitais sintéticas, podendo ser utilizado sem nenhum custo para criar pequenos bancos de dados de impressões digitais, através da opção “*Generate*” que gera as impressão digitais uma por uma.

3.2.5 – Qualidade da Imagem

A qualidade da imagem é um dos fatores mais importantes no processo de comparação, seja ele por uso de computador ou realizado de forma manual. Mas, a qualidade das imagens de impressões digitais ao serem adquiridas geralmente não é satisfatória. Isso torna o pré-processamento uma etapa crucial em um sistema de reconhecimento que utilize impressões digitais.

O pré-processamento de imagens envolve a transformação e análise de imagens através do computador visando melhorar suas características visuais, tais como contraste e eliminação de ruídos, além de extrair regiões de interesse para a representação de objetos contidos nas imagens (FARIA, 2005).

A aplicação do filtro de contraste é uma das técnicas utilizadas no processo de melhoria de qualidade da imagem, cujo objetivo principal é aumentar a capacidade de distinção visual entre os objetos contidos na mesma. No caso das impressões digitais, aumenta a distinção entre as cristas e vales. O filtro de contraste calcula para cada *pixel* um valor médio de intensidade em uma vizinhança. Se o valor do *pixel* for menor que a média do bloco considerado, então o *pixel* de interesse receberá valor zero; caso contrário o *pixel* manterá seu valor original (COSTA, 2001). É possível perceber o resultado da aplicação do filtro de contraste observando a figura 46.

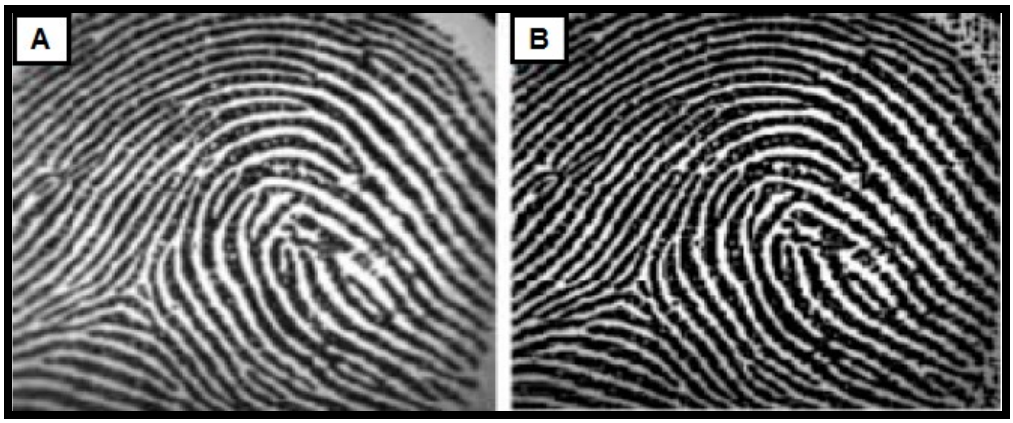

Figura 46 – Filtro de contraste. (A) imagem original e (B) imagem filtrada (COSTA, 2001)

Outra técnica utilizada na etapa de pré-processamento é a binarização, que consiste em transformar os tons de cinza da imagem em preto e branco, ou seja, transformar os tons de cinza em uma imagem binária de zeros e uns. A binarização é uma etapa muito importante, pois se for mal executada pode gerar perda de informação.

A classificação dos *pixels* da imagem quanto ao valor binário é feita a partir de um limiar chamado nível de *threshold*. O valor de intensidade de cada *pixel* é verificado para decidir se ele receberá o valor 0 correspondente ao preto ou valor 1 correspondente ao branco. Se o *pixel* analisado tem valor menor ou igual ao limiar, então recebe valor equivalente a preto, caso contrário o valor recebido é equivalente a branco (FARIA, 2005). A figura 47 ilustra o resultado do processo de binarização de uma imagem de impressão digital.

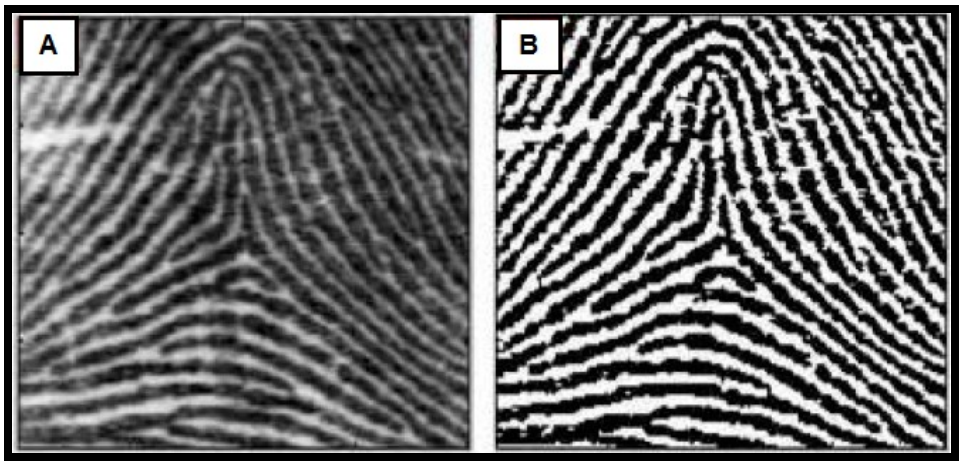

Figura 47 – Binarização. (A) imagem original e (B) imagem binarizada (COSTA, 2001)

Outro processo que torna mais fácil a extração de minúcias das imagens de impressões digitais é o afinamento ou esqueletização que reduz a largura das cristas a um *pixel*. O processo também conhecido com *thinning* é uma técnica utilizada para remover *pixels* indesejáveis sem que ocorram alterações na estrutura da imagem.

O algoritmo de afinamento analisa a imagem da impressão digital e remove os *pixels* redundantes das linhas que formam as cristas. Esse processo é repetido até que não se tenha mais *pixels* redundantes, resultando no esqueleto da imagem. A varredura da imagem é feita linha a linha, examinando a vizinhança e verificando se o *pixel* pode ou não ser apagado (MAZI, 2009). A figura 48 mostra o processo de afinamento da imagem.

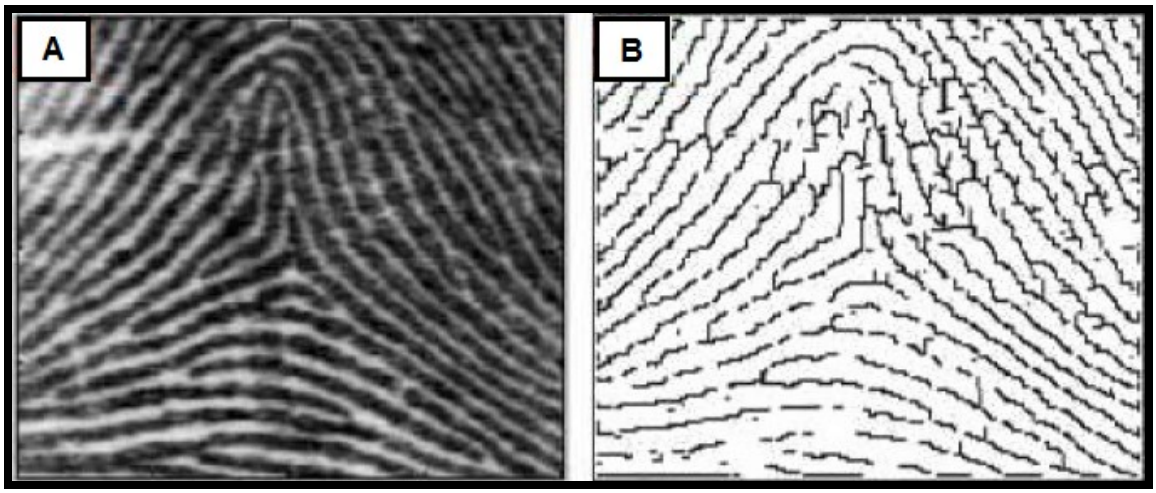

Figura 48 – Afinamento. (A) imagem original e (B) imagem afinada (COSTA, 2001)

O pré-processamento visando o tratamento da imagem é importante, pois objetiva a melhora de qualidade e o preparo da imagem obtida no processo de aquisição para que o sistema identifique as minúcias com maior facilidade e precisão.

3.2.6 – Ponto de Referência

A base de partida para a extração de características em uma impressão digital é o ponto de referência. Existem diversos pontos que podem ser utilizados como referência, bastando que o mesmo seja necessariamente distinto do resto da imagem e de fácil identificação na mesma.

Um dos critérios utilizado para determinar o ponto de referência é localizar o ponto de maior curvatura côncava (PRABHAKAR, 2001). Observando a figura 49 é possível perceber a localização do ponto de referência em uma imagem de impressão digital utilizando esse critério.

Figura 49 – Ponto de referência (PRABHAKAR, 2001)

O ponto de referência numa impressão digital tem que ser único e não deve existir ambiguidade na sua detecção, pois é a partir do ponto de referência que é determinada a localização de cada minúcia dentro da impressão digital. Sendo assim, imagens de uma mesma impressão devem ter sempre a mesma localização para o ponto de referência dentro da imagem.

3.2.7 – Extração de Minúcias

A unicidade de uma impressão digital é garantida por meio das propriedades das minúcias nela encontrada, por isso são características fundamentais no reconhecimento de impressões digitais.

O processo de extração de minúcias não pode ser realizado diretamente com imagens obtidas em tempo real porque estas não apresentam bons níveis de qualidade. Por esse motivo, torna-se necessário efetuar o pré-processamento da imagem, obtendo assim os níveis de qualidade exigidos.

Considerando que após o pré-processamento as cristas que compõem a impressão digital apresentam um conjunto de linhas com espessura de um *pixel*, a extração de minúcias resume-se a procurar determinados padrões sobre essas linhas. Esses padrões consistem em blocos de dimensões 3x3 que definem numa imagem binária

as combinações que representam minúcias do tipo terminação, quando o *pixel* central apresenta um único vizinho, e bifurcação quando ele apresenta três vizinhos (MAZI, 2009). A figura 50 ilustra a representação de uma minúcia do tipo terminação e outra do tipo bifurcação.

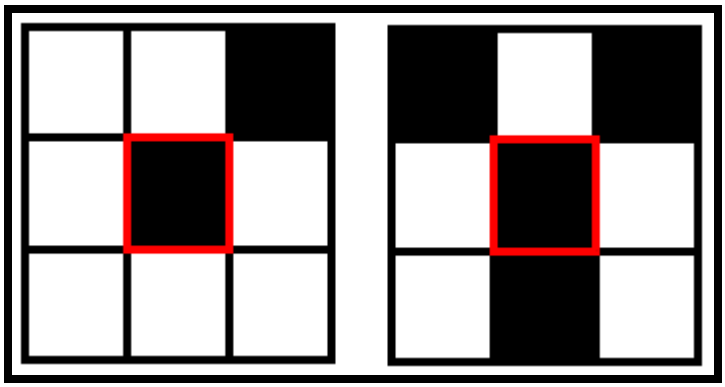

Figura 50 – Esquerda terminação e direita bifurcação.

Essa técnica, denominada de *Crossing Number* (CN), permite determinar as propriedades de um *pixel* simplesmente contando o número de transições em preto e branco existente nas 8-vizinhanças do *pixel* que está sendo processado (COSTA, 2001). O CN de um *pixel P* é dado pela eq.(11):

$$CN = 0.5 \sum |P_i - P_{i+1}| \quad , \tag{11}$$

em que P_i é o valor do *pixel* na vizinhança de *P*. O índice *i* é um ciclo de período 8, ou seja, *P8 = P0*. Para um *pixel P*, considera-se os 8 vizinhos em uma vizinhança 3x3, podendo cada um ter valores diferentes (0 ou 1). Na figura 51 é mostrada a vizinhança 3x3 do ponto *P* para o cálculo do CN.

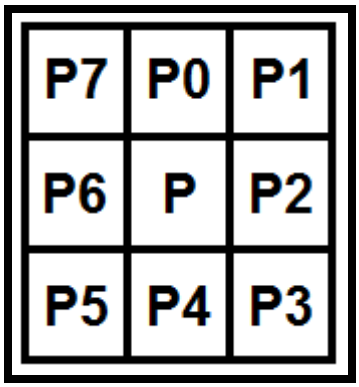

Figura 51 – Cálculo do CN

As minúcias do tipo terminação e bifurcação são encontradas utilizando-se as propriedades do CN. O valor obtido (CN) indica a propriedade do *pixel* de acordo com a tabela 6.

Propriedades do CN	Minúcias
0	Ponto Isolado
1	Terminação
2	Ponto Contínuo
3	Bifurcação
4	Ponto de Cruzamento

Tabela 6 – Propriedades do *pixel* CN (COSTA, 2001)

Para evitar a localização de falsas minúcias decorrentes de sua posição junto à borda da imagem, o processo de extração percorre apenas uma região de interesse, a qual se apresenta como sendo a área em torno do ponto de referência. Normalmente, é considerada como região de interesse todos os pontos em que a distância ao ponto de referência é inferior a 100 *pixels*. Dessa forma, todos os pontos identificados de forma errada como minúcias devido a se encontrarem na extremidade da impressão digital são ignorados.

O processo de extração de minúcias percorre a região de interesse a procura dos padrões característicos: terminações e bifurcações. Sempre que encontra um destes padrões, extrai a informações e cria uma entrada no vetor de características com a posição, o tipo da minúcia e o ângulo formado.

Para que uma impressão digital seja considerada igual à outra, existe um número mínimo de minúcias iguais que têm de ser encontradas. Quanto mais minúcias forem consideradas, mais baixa é a probabilidade das impressões serem consideradas iguais quando na realidade são diferentes, evitando-se assim a falsa aceitação (PACHECO, 2003).

4 – DESENVOLVIMENTO DO TRABALHO

Neste capítulo será apresentada a elaboração do estudo de caso para a aplicação dos conceitos obtidos durante a revisão bibliográfica. É apresentada também a modelagem do problema, bem como os métodos utilizados para obter a solução.

4.1 – DESCRIÇÃO DO PROBLEMA

Neste projeto foi desenvolvido um sistema biométrico que utiliza dois procedimentos de reconhecimento. O primeiro é quando o usuário se apresenta como sendo uma determinada pessoa e o sistema compara a autenticidade da informação. O segundo, é quando a identificação de um usuário ocorre a partir do dado biométrico dele e, então, se faz uma busca no banco de dados, comparando as informações até que seja encontrado ou não um registro idêntico ao que está sendo procurado.

4.2 – MODELAGEM DO PROBLEMA

Os sistemas biométricos podem operar realizando autenticação ou identificação dos usuários. Na autenticação o usuário tem sua impressão digital previamente registrada e posteriormente, sempre que o mesmo desejar ser autenticado, informa sua identidade juntamente com uma amostra de sua impressão digital. Uma comparação com o padrão correspondente a sua identidade que está armazenado na base de dados é realizada. Se a semelhança entre elas estiver dentro de uma faixa determinada, o usuário é então autenticado.

A parte principal do projeto foi desenvolver a segunda parte do aplicativo, cujo cenário é um pouco mais complexo, pois além da aquisição da impressão digital é necessário também realizar uma comparação com todos os registros da base de

dados até que se encontre um padrão que apresente a semelhança exigida para se obter a identificação. Essa etapa adicional é necessária devido ao fato de o usuário não informar sua identidade no momento da identificação, bastando apenas que esse apresente sua amostra biométrica. Isso pode acarretar em a pessoa a ser identificada nem estar cadastrada na base de dados. A figura 52 mostra a modelagem bem simplificada do sistema biométrico.

Figura 52 – Visão geral do sistema

Visando facilitar o desenvolvimento do projeto, o problema foi dividido em três módulos: capturar e pré-processar imagem, extrair minúcias e gerar modelo, buscar e comparar modelos.

4.2.1 – Módulo 1: Capturar e Pré-Processar Imagem

As imagens utilizadas em sistemas de reconhecimento de impressões digitais normalmente são adquiridas por sensores. Entretanto, o processo de captura das imagens de impressão digital utilizadas pelo sistema desenvolvido, foi realizado a partir do aplicativo *SFinGe*. Este aplicativo é uma versão demonstrativa, na qual é possível gerar automaticamente imagens de impressão digital sintética de excelente qualidade diretamente em tons de cinza.

Antes de se extrair as características biométricas da impressão digital é necessária uma fase de preparação ou pré-processamento da imagem, que consiste basicamente na aplicação de filtros que melhorem ou realcem qualidades presentes nas imagens de forma a facilitar os processos seguintes de extração de características e comparação. Como as imagens utilizadas pelo sistema foram obtidas de forma sintética, não foi necessário aplicar nem um filtro para a eliminação de ruídos, nem mesmo para aumento de contraste, uma vez que esse tipo de imagem já apresenta ótima qualidade.

Dessa forma, a etapa de pré-processamento resumiu-se em aplicar o processo de binarização ou limiarização, que é a conversão da imagem em tons de cinza para uma imagem binária com somente dois tons, branco e preto, e em seguida, o afinamento ou esqueletização da imagem que tem como objetivo reduzir a quantidade de pontos da imagem mantendo a formação original. Após esse processo, a estrutura da imagem passa a possui a espessura de apenas um *pixel*, o que torna muito mais fácil o processo de extração de características.

4.2.2 – Módulo 2: Extrair Minúcias e Gerar Modelo

De posse da imagem afinada ocorre o processo de extração das minúcias através de análise de vizinhança. A técnica utilizada para a detecção das minúcias foi o *Crossing Number* que determina se um *pixel* é uma minúcia simplesmente contando o número de transições em preto e branco existente nas 8-vizinhanças do *pixel* que está sendo processado, de forma que se o *pixel* da imagem possuir apenas um vizinho é considerado minúcia do tipo terminal, se possuir três vizinhos é bifurcação.

Cada minúcia detectada foi caracterizada pelo seu tipo, terminação ou bifurcação e por suas coordenadas (*x, y)* relativas na imagem. O processo de extração de minúcias percorre a imagem e a cada nova minúcia encontrada extrai a sua posição e cria uma entrada no vetor de características gerando assim o modelo biométrico a ser armazenado ou comparado.

Para evitar a detecção de falsas minúcias, que se encontravam nas bordas da imagem, foi definida uma área delimitadora para encontrar somente as minúcias mais internas, ignorando as extremidades da impressão digital.

4.2.3 – Módulo 3: Buscar e Comparar Modelos

Esta etapa do processo compara os dados biométricos da impressão digital obtida pelos passos descritos anteriormente com os dados de outras armazenadas na base de dados, avaliando a semelhança entre elas. O objetivo principal desta etapa é determinar se a impressão digital fornecida pertence a alguma pessoa que foi anteriormente cadastrada.

O algoritmo de comparação se baseia nas informações do modelo gerado como a localização e tipo de cada minúcia identificada durante a etapa anterior, verificando se é equivalente a alguma que está armazenada. Assim sendo, quanto maior o número de minúcias correspondentes entre os modelos, maior a probabilidade de pertencerem à mesma pessoa.

4.3 – ESPECIFICAÇÃO

Foi utilizada uma metodologia orientada a objetos no processo de especificação do sistema biométrico desenvolvido. Tal especificação está representada em diagramas elaborados com o uso da ferramenta ArgoUML, inteiramente escrita em Java e uma das principais ferramentas *open source* de modelagem UML (*Unified Modeling Language*) que inclui suporte para a maioria dos diagramas UML 1.4 padrão.

Na especificação foram incluídos os diagramas de casos de uso, diagrama de classes, os diagramas de sequência e o diagrama de atividade.

4.3.1 – Diagrama de Casos de Uso

O Diagrama de Casos de Uso é uma técnica de modelagem usada para descrever o que um sistema deve fazer definindo seus requisitos funcionais. A figura 53 ilustra o Diagrama de Casos de Uso descrevendo as três funcionalidades do sistema biométrico:

- **Manter Indivíduos**: é a funcionalidade responsável por incluir, alterar, remover e procurar indivíduos bem como as características de suas impressões digitais;
- **Autenticar Indivíduos**: é a funcionalidade responsável por verificar a autenticidade das informações fornecidas pelo usuário, de forma a confirmar sua identidade;
- **Identificar Indivíduos**: é a funcionalidade responsável por procurar e estabelecer a identidade do usuário.

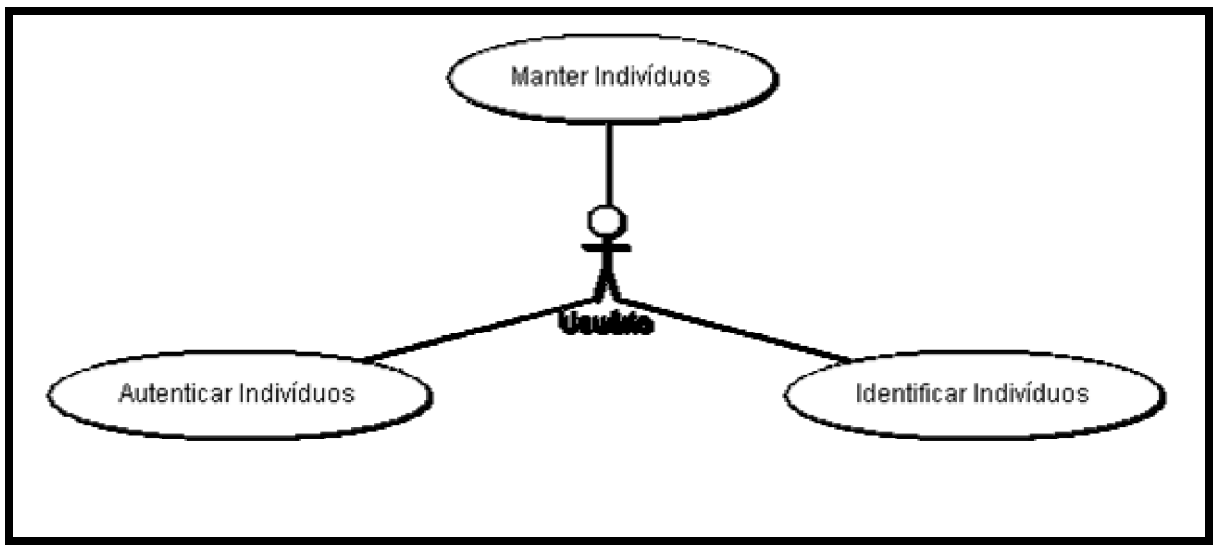

Figura 53 – Diagrama de Casos de Uso

4.3.2 – Diagrama de Classes

O Diagrama de Classes descreve a estrutura estática do sistema em termos de classes e relacionamentos entre elas, onde estas representam os objetos que são gerenciados pela aplicação. No desenvolvimento desse trabalho, as classes foram divididas em pacotes para uma melhor organização e entendimento do código.

4.3.2.1 – Pacote *beans*

No pacote *beans* estão agrupadas as classes que representam as entidades do sistema e permitem a manipulação de suas informações. Os atributos de cada entidade são encapsulados de modo que estes fiquem acessíveis apenas através dos métodos *setters* e *getters*. Na figura 54 são apresentadas as três entidades utilizadas pelo sistema biométrico juntamente com seus atributos:

- **Pessoa**: classe responsável por representar os objetos da entidade pessoa;
- **ImpressaoDigital**: classe responsável por representar os objetos da entidade impressão digital;
- **Minucia**: classe responsável por representar os objetos da entidade minúcia.

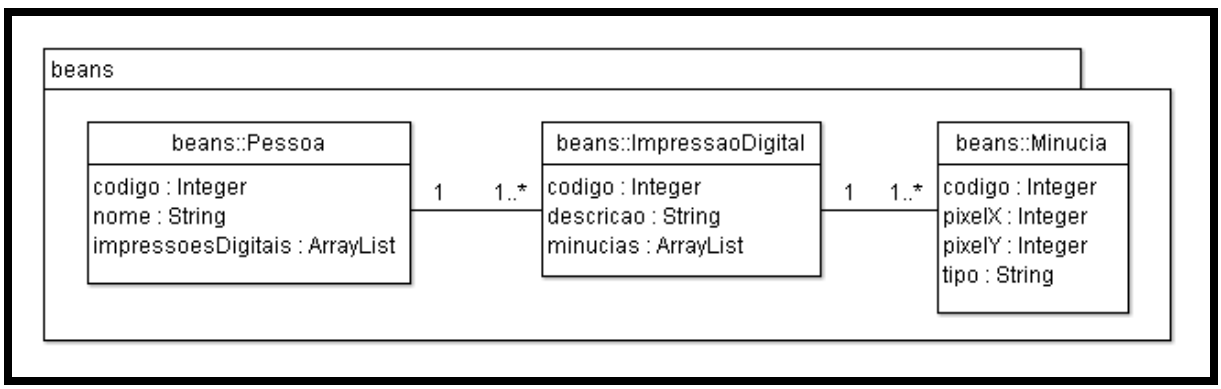

Figura 54 – Diagrama de Classes Pacote *beans*

Os métodos *setters* e *getters* foram omitidos apenas para uma melhor visualização da estrutura e relacionamento dentre as classes, porém eles estão presentes em cada um dos atributos de cada classe.

4.3.2.2 – Pacote dao

No pacote DAO *(Data Access Object)* estão agrupadas as classes que efetuam o tratamento e manipulação das informações providas do Sistema Gerenciador de Banco de Dados. Assim, todo o trabalho relacionado com o acesso ao banco de dados é abstraído e encapsulado, sendo que as classes que necessitem manipular os dados simplesmente devem conhecer a classe DAO, sem se preocupar com abrir e fechar conexão ou inserir comandos. A figura 55 ilustra a estrutura das classes do pacote DAO:

- **PessoaDAO**: classe responsável por realizar a ligação entre os objetos da classe Pessoa do pacote *bean* com o banco de dados, realizando todas as operações necessárias de acesso e manipulação de dados referente a entidade pessoa;
- **ImpressaoDigitalDAO**: classe responsável por realizar a ligação entre os objetos da classe ImpressaoDigital do pacote *bean* com o banco de dados, realizando todas as operações necessárias de acesso e manipulação de dados referente a entidade impressão digital;
- **MinuciaDAO**: classe responsável por realizar a ligação entre os objetos da classe Minucia do pacote *bean* com o banco de dados, realizando todas as operações necessárias de acesso e manipulação de dados referente a entidade minúcia;
- **IdentificarDAO**: classe responsável por estabelecer o acesso ao banco de dados e realizar toda a manipulação de dados necessária para a realização do processo de identificação dos indivíduos a partir das impressões digitais.

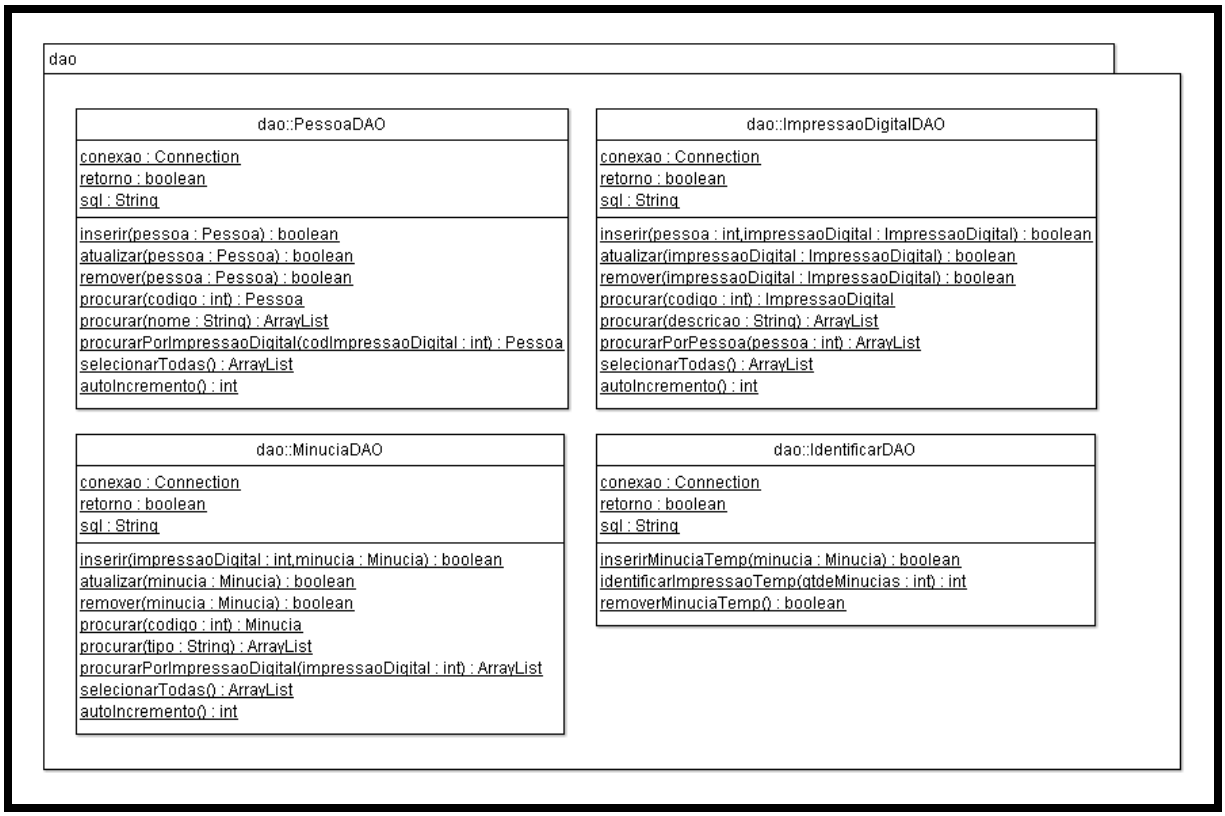

Figura 55 – Diagrama de Classes Pacote DAO

4.3.2.3 – Pacote util

É no pacote util que estão agrupadas as classes que, de alguma forma, podem ser utilizadas em várias etapas do sistema para a execução de operações específicas ao sistema biométrico de reconhecimento de impressões digitais. A figura 56 descreve as classes do pacote util:

- **Evento**: classe utilizada para executar as três funcionalidades disponibilizadas pelo sistema biométrico: cadastrar um indivíduo juntamente com suas impressões digitais e as respectivas características biométricas, autenticar a identidade de um indivíduo que diz ser determinada pessoa e identificar um indivíduo através da análise da impressão digital por ele apresentada ao sistema;

- **ProcessamentoDeImagem**: é a principal classe do sistema biométrico, pois é nela que se encontram todas operações de processamento e manipulação das imagens de impressões digitais utilizadas pelo sistema desenvolvido. Dentre as operações disponibilizadas por esta classe então a binarização e o afinamento da imagem, bem como a localização e extração das minúcias que compõe o modelo biométrico.

Figura 56 – Diagrama de Classes Pacote util

Além dos pacotes apresentados anteriormente, o projeto é composto por mais outros dois pacotes: o pacote db, onde se encontra a classe ConexaoDB responsável por estabelecer a conexão entre o sistema biométrico e o banco de

dados; e o pacote *view*, onde estão agrupadas as classes responsável pela construção das interfaces, possibilitando a comunicação e a interação entre o usuário e o sistema.

4.3.3 – Diagrama de Sequência

A colaboração dinâmica entre os vários objetos do sistema é mostrada no Diagrama de Sequência. Ele mostra a interação entre os objetos, sendo possível perceber a sequência ou ordem temporal em que as mensagens são trocadas entre eles durante a execução de um determinado processo. Foi elaborado um Diagrama de Sequência para cada Caso de Uso especificado:

4.3.3.1 – Manter Indivíduos

A sequência de ações representadas no diagrama da figura 57 é executada sempre que um dos processos relativos à manutenção de registro (inserir, alterar, excluir e pesquisar) de indivíduos for necessária. É possível perceber como ocorre a comunição entre as várias classes envolvidas neste processo, em especial, a ação de inserir novos indivíduos que é o processo mais complexo deste caso de uso.

Foi ocultada no diagrama a comunicação existente entre as classes PessoaDAO e ImpressaoDigitalDAO, bem como a comunicação existente entre as classes ImpressaoDigitalDAO e MinuciaDAO, não só no processo de inserção como também nos processos de atualização, remoção e procura de objetos da classe Pessoa. Entretanto, a comunicações entre estas classes acontecem sempre que um objeto da classe Pessoa é inserido, atualizado, pesquisado ou removido da base de dados do sistema. As comunicações existes entre as classes Pessoa e ImpressaoDigital e entre as classes ImpressaoDigital e Minucia também foram ocultadas para uma melhor visualização das trocas de mensagens mais importantes durante a execução dos processos.

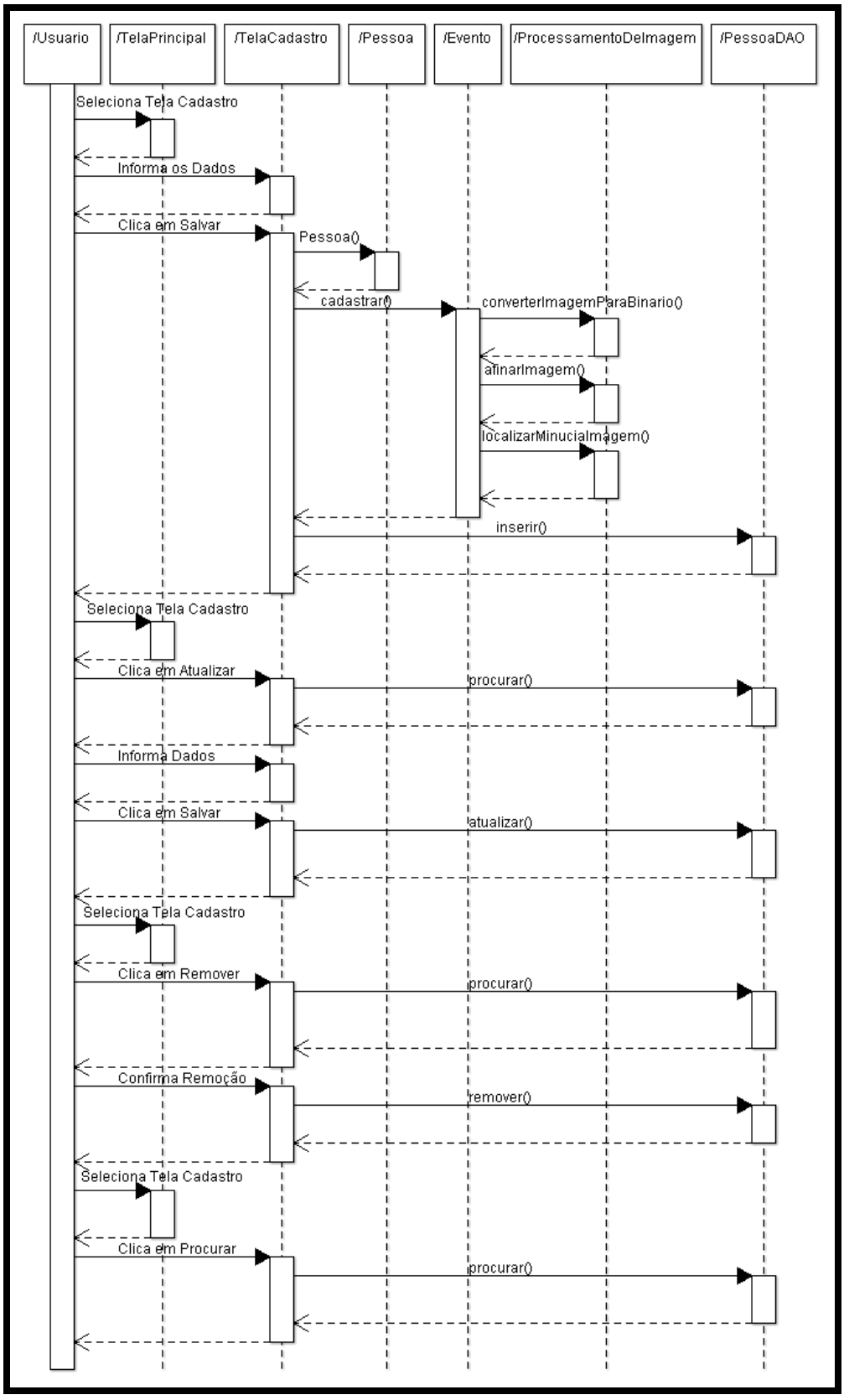

Figura 57 – Diagrama de Sequência Manter Indivíduos

4.3.3.2 – Autenticar Indivíduos

O diagrama mostrado na figura 58 apresenta a sequência de ações realizadas durante a execução do caso de uso Autenticar Indivíduos, o qual é utilizado para determinar se realmente o indivíduo é quem diz ser.

Da mesma forma como no diagrama anterior, a comunicação existente entre as classes PessoaDAO e ImpressaoDigitalDAO e entre as classes ImpressaoDigitalDAO e MinuciaDAO foram ocultadas neste diagrama.

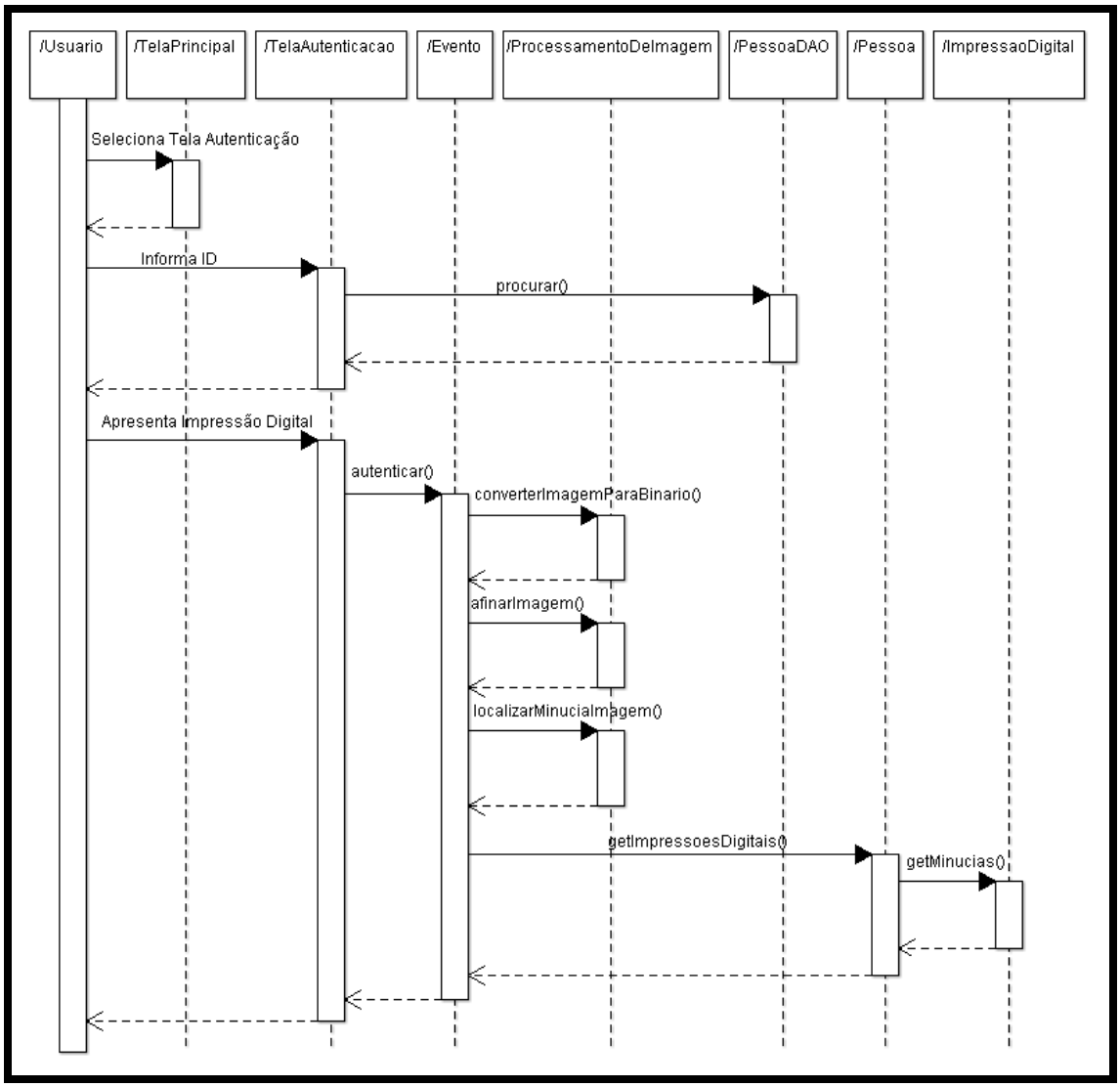

Figura 58 – Diagrama de Sequência Autenticar Indivíduos

4.3.3.3 – Identificar Indivíduos

A figura 59 apresenta o diagrama ilustrando a sequência de ações necessárias para a execução do caso de uso Identificar Indivíduos, o qual determinar a identidade do indivíduo a partir de sua impressão digital.

Neste diagrama também foi ocultada a comunicação existente entre as classes PessoaDAO e ImpressaoDigitalDAO e entre as classes ImpressaoDigitalDAO e MinuciaDAO.

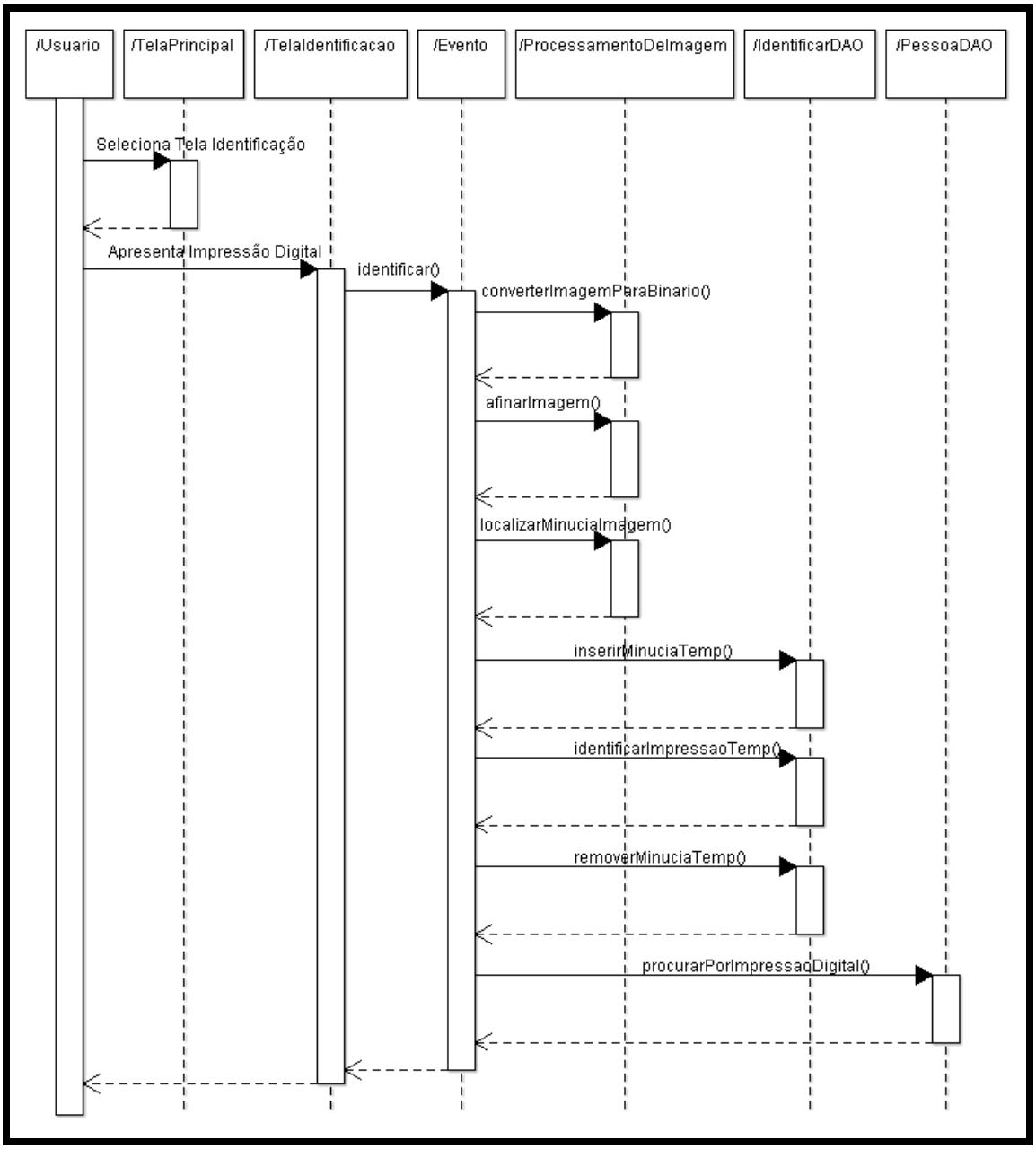

Figura 59 – Diagrama de Sequência Identificar Indivíduos

4.3.4 – Diagrama de Atividades

O objetivo do Diagrama de Atividades é mostrar o fluxo de atividades em um único processo, mostrando como uma atividade depende da outra. Na figura 60 é ilustrado o Diagrama de Atividades do sistema biométrico, onde é possível observar, de forma

clara, todos os passos necessários para a realização de cada uma de suas funcionalidades.

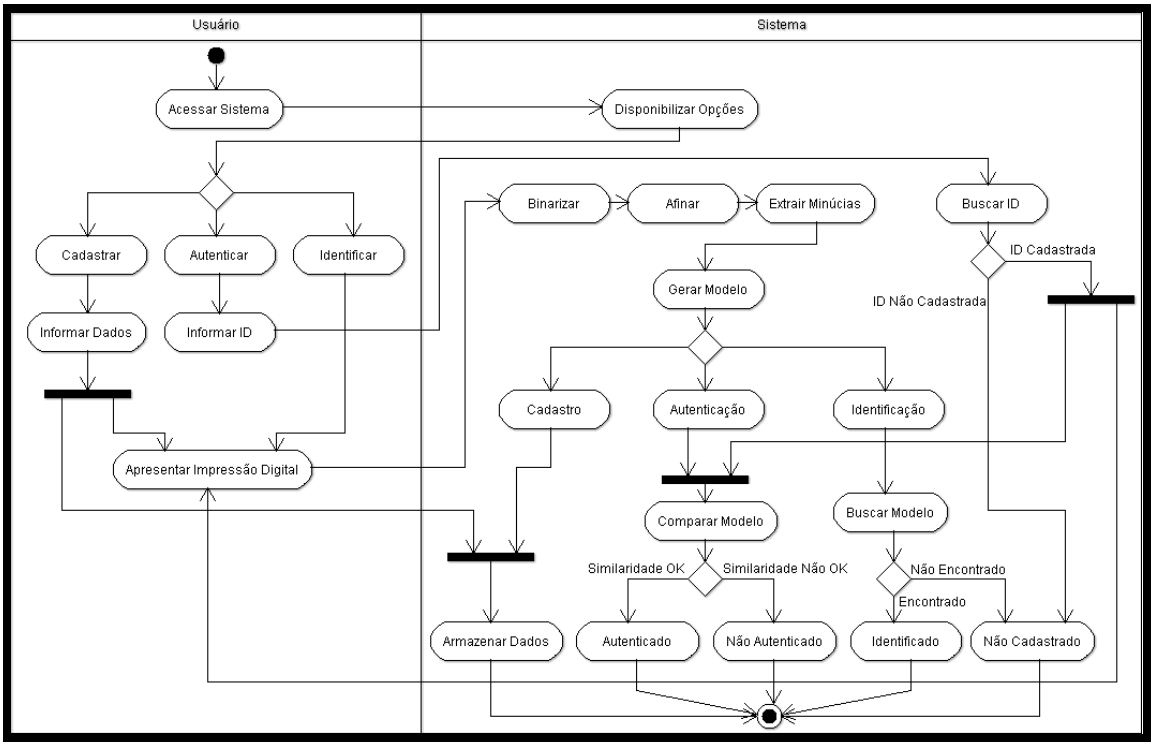

Figura 60 – Diagrama de Atividades

4.4 – IMPLEMENTAÇÃO DO APLICATIVO

Nesta seção é apresentada, com mais detalhes, os métodos utilizados na implementação do sistema biométrico desenvolvido neste projeto.

4.4.1 – Metodologia Utilizada

A implementação do aplicativo envolveu as etapas de pré-processamento das imagens de impressão digital onde estas são binarizadas e afinadas. Também foram implementadas as etapas de extração de características, autenticação e

identificação das impressões digitais. A metodologia utilizada em cada etapa é descrita nesta subseção. O sistema foi implementado na linguagem de programação Java com a utilização do ambiente integrado de desenvolvimento (*IDE – Integrated Development Environment*) *NetBeans IDE 6.9.1*. Para criar a base de dados de impressões digitais foi utilizado o aplicativo *SFinGe*.

4.4.1.1 – Processo de Binarização

Na primeira etapa do pré-processamento foi feita a conversão da imagem original em escala de cinza para uma imagem binária, com apenas duas tonalidades, branco e preto. No sistema implementado foi utilizada a técnica de binarização global, ou seja, apenas um nível de *threshold* é utilizado para binarizar toda a imagem. Esse método foi escolhido porque o conteúdo das imagens de impressão digital processadas nesse trabalho são basicamente bimodais. O *threshold* escolhido foi 45, pois foi observado que sendo a imagem bimodal, qualquer valor próximo a 45 consegue separar os objetos do fundo sem que ocorra perda de informações. A figura 61 apresenta o resultado da binarização aplicada à imagem original.

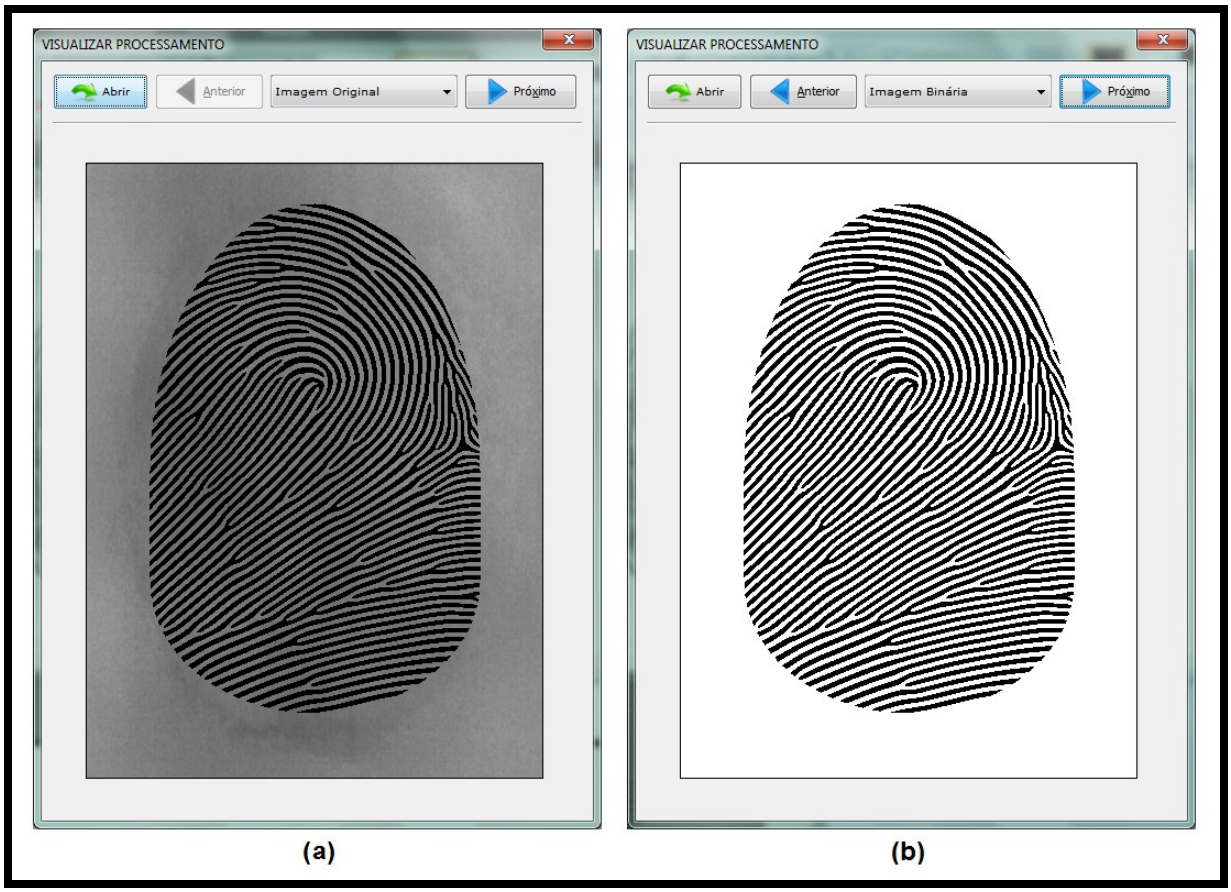

Figura 61 – (a) imagem original e (b) imagem binária

Pelo fato do fundo da imagem original apresentar grandes variações de níveis de cinza, o método de binarização local não foi satisfatório, pois algumas partes do fundo ficaram pretas confundindo-se com as linhas. Dessa forma foi adotada a limiarização global.

4.4.1.2 – Afinamento

Após a binarização da imagem, a próxima etapa é obter o esqueleto com a estrutura das linhas que compõem a impressão digital. O método escolhido para o afinamento da imagem binarizada foi o método de Zhang e Suen, pois apresentou bons resultados mantendo as linhas da impressão digital com sua estrutura original. Esta

é uma característica muito importante no afinamento, pois se o esqueleto gerado apresentar falhas, estas se tornarão falsas minúcias no processo de extração de características. A figura 62 apresenta o resultado do afinamento da imagem binária.

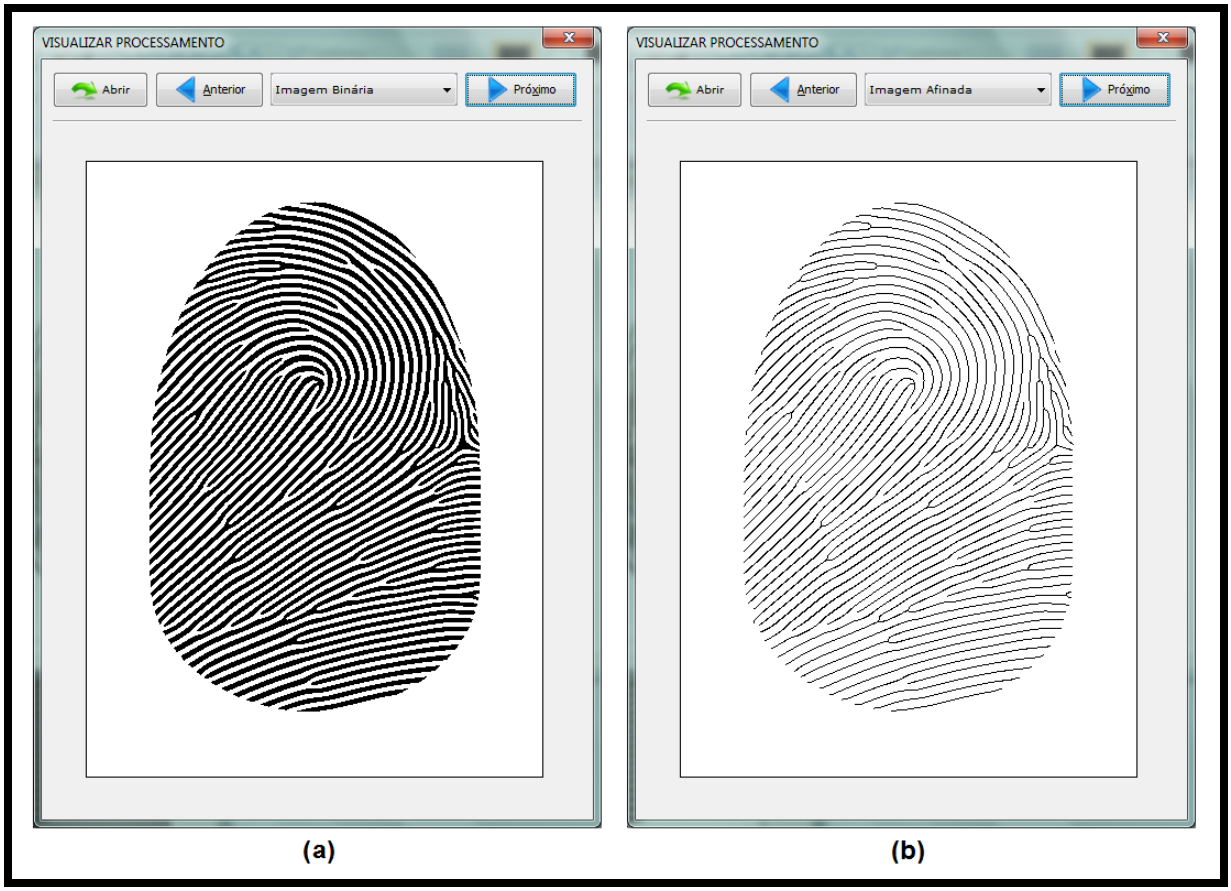

Figura 62 – (a) imagem binária e (b) imagem afinada

Entretanto, ao final da esqueletização, é possível perceber algumas áreas formadas por estruturas semelhantes a uma escada. Tais estruturas apresentam *pixels* cuja remoção não torna as linhas descontinuas, porém facilita muito o processo de localização das minúcias. Por conta disso, foi utilizada a técnica de limpeza do esqueleto. Este método remove todo formato de serrilhamento da imagem afinada. A diferença entre as imagens afinada antes e após a limpeza do esqueleto pode ser observada na figura 63.

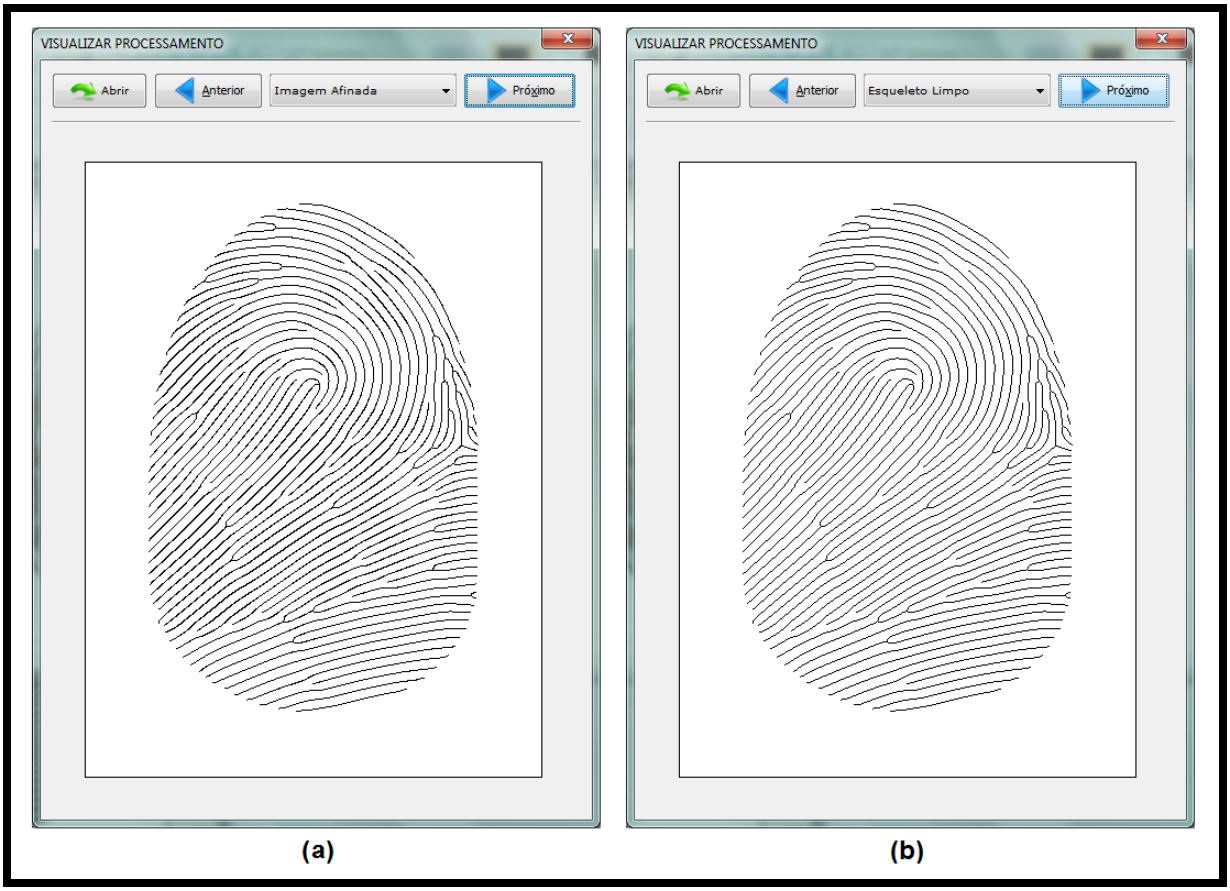

Figura 63 – (a) imagem afinada e (b) esqueleto limpo

Uma imagem gerada com a afinação de Zhang e Suen necessita posteriormente passar pela técnica de *staircase removal*, pois assim pode apresentar melhores resultado para o afinamento.

4.4.1.3 – Extração de Características

De posse da imagem afinada cujas linhas apresentam apenas um *pixel* de espessura, é iniciado o processo de extração de características, ou seja, a geração do modelo biométrico que será utilizado no cadastro dos indivíduos, bem como para realizar sua autenticação ou identificação.

Neste processo foi utilizada a técnica de *Crossing Number* para localizar as minúcias do tipo terminação e bifurcação. De cada *pixel* identificado como sendo uma minúcia obtém sua localização, ou seja, a coordenada (*x, y)* e seu tipo. Essas informações são então inseridas no banco de dados formando o modelo biométrico para o referido indivíduo. Na figura 64 é mostrada uma impressão digital com a localização das minúcias. As bifurcações foram destacadas por um pequeno quadrado enquanto que um círculo foi desenhado para realçar as terminações.

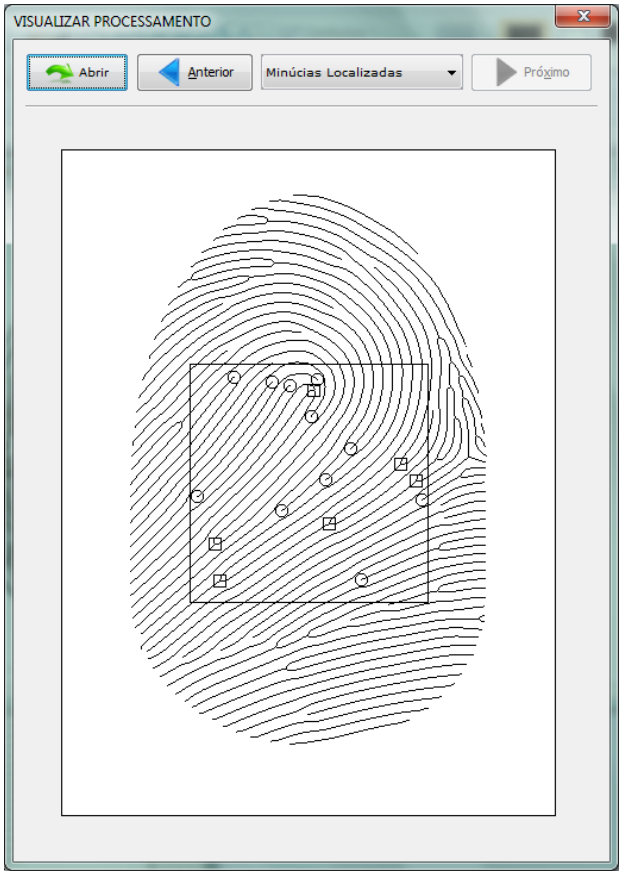

Figura 64 – Minúcias Localizadas

Para evitar a identificação das falsas minúcias localizadas nas extremidades da imagem, uma área de interesse foi definida de forma a analisar somente a região central das impressões digitais. A delimitação desta área abrange uma região de 200 x 200 *pixels,* com o centro correspondente ao centro da imagem, como

mostrado na figura 64. A geração do modelo biométrico é utilizada tanto no processo de cadastro quanto nos processos de autenticação ou identificação dos indivíduos.

4.4.1.4 – Autenticação e Identificação das Impressões Digitais

É comum que os sistemas biométricos apresentem alguma taxa de erro, seja pela falsa aceitação ou pela falsa rejeição, entretanto, no sistema desenvolvido, como as imagens utilizadas na realização do cadastro são as mesmas utilizadas nos processos de autenticação e identificação, a probabilidade de ocorrer algum erro é muito pequena. Diante disso, a taxa de similaridade exigida entre os modelos tanto na autenticação quanto na determinação da identidade é de 100%, ou seja, elas devem ser exatamente iguais. É importante ressaltar que tal condição não se aplica em sistemas que utilizam imagens adquiridas por outros meios citados neste trabalho.

Neste contexto, a autenticação de um indivíduo se dá pela recuperação do modelo biométrico armazenado e pela confrontação com o modelo biométrico gerado a partir da impressão digital apresentada no instante da autenticação. Se os modelos forem considerados iguais, a autenticação é positiva, caso contrário à identidade não é autenticada.

Na determinação da identidade, lançou-se mão de uma técnica um pouco mais complexa. A impressão digital apresentada no momento da identificação é utilizada na geração de um modelo biométrico. Uma busca é realizada na base de dados selecionando todas as minúcias que são equivalentes às contidas no modelo gerado, ou seja, todas as minúcias que são do mesmo tipo e estão localizadas nas mesmas coordenadas. Quando todas as minúcias do modelo forem processadas, as minúcias selecionadas são agrupadas de acordo com o modelo a que pertencem. O modelo que for composto pelo maior número de minúcias equivalentes é então localizado. Para estabelecer a identidade basta verificar se a similaridade exigida entre os modelos foi alcançada, e então, buscar a quem pertence o modelo localizado.

4.4.2 – Operacionalidade da Implementação

Para contornar a dificuldade de acesso a um dispositivo real de aquisição de impressões digitais, um conjunto de amostras de imagens sintéticas foi gerado usando o aplicativo *SFinGe* que, apesar de oferecer a opção de adicionar ruídos, distorções, rotação e translação no processo de geração das imagens, estas não foram utilizadas, pois tais questões não foram tratadas na implementação deste trabalho. A figura 65 mostra imagens de impressões digitais geradas pelo *SFinGe* com adição de ruído. Além disso, a impressão digital mostrada à esquerda apresenta uma rotação de -10° enquanto que a mostrada à direita apresenta rotação de 10°.

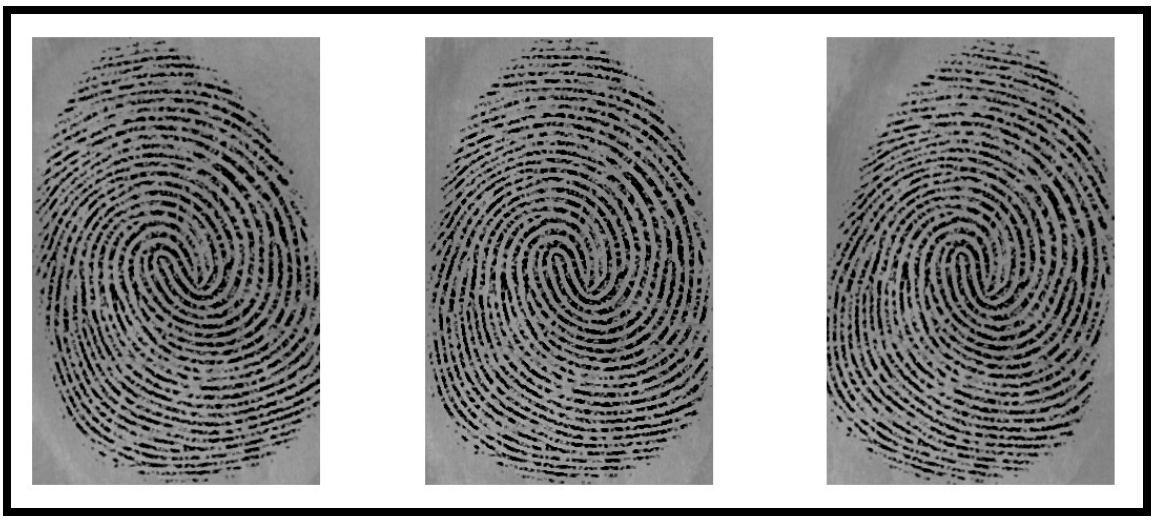

Figura 65 – Impressões digitais geradas com ruído

No sistema desenvolvido não foi tratado problemas quanto a imagens de má qualidade, rotação e translação que podem ocorrer durante o processo de aquisição em um sensor real. Assim, para utilizar as funcionalidades disponibilizadas pelo sistema, sempre que for solicitada a apresentação de uma impressão digital, o usuário simplesmente escolhe uma das impressões digitais sintéticas geradas previamente. A figura 66 mostra a interface inicial do sistema desenvolvido.

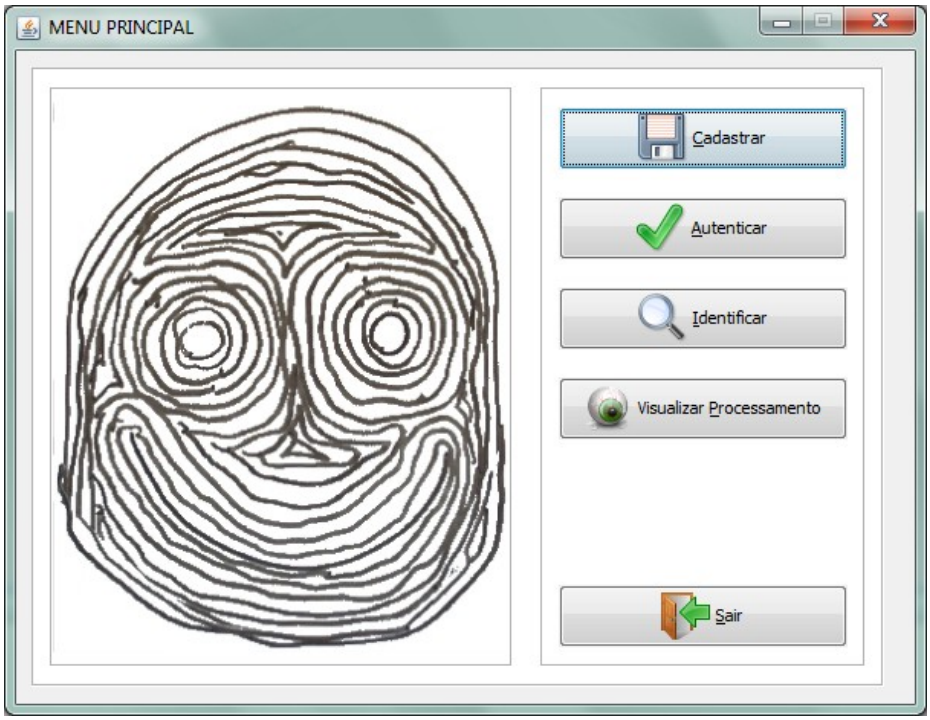

Figura 66 – Interface inicial do sistema

4.4.2.1 – Implementação do Caso de Uso Manter Indivíduos

O caso de uso “Manter Indivíduos” é executado principalmente para adicionar novas pessoas à base de dados biométrica. É executando também para alterar ou remover os dados de uma pessoa que já tenha sido cadastrada anteriormente. O acesso a este caso de uso é feito através do botão “Cadastrar” disponível no Menu Principal do sistema.

Para inserir um novo registro, o usuário primeiramente informa o nome do indivíduo e em seguida apresenta uma ou mais impressões digitais juntamente com a descrição a qual dedo pertence cada impressão. Logo após, basta confirmar a inclusão, clicando no botão “Confirmar”. Diante disso, o sistema gera um modelo biométrico para cada impressão digital apresentada e armazena na base de dados, exibindo uma mensagem para o usuário. A figura 67 mostra a interface de cadastro.

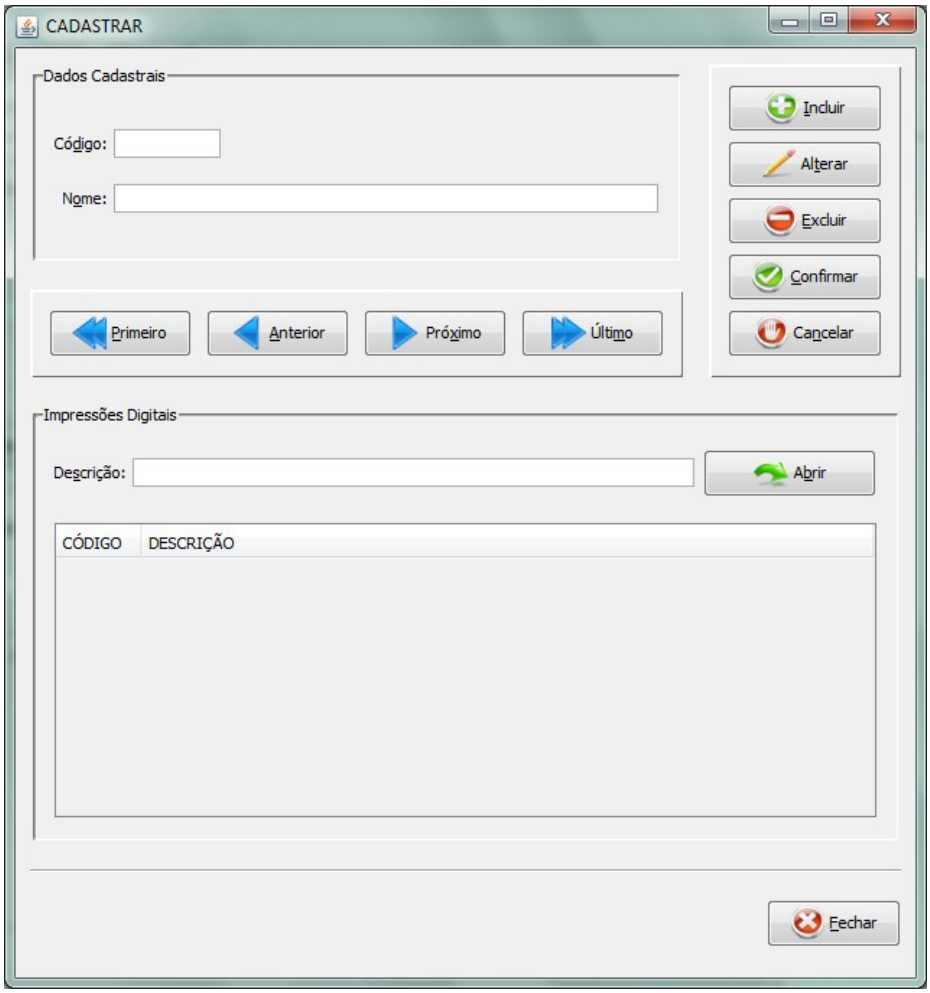

Figura 67 – Interface de cadastro

Caso seja necessário excluir ou alterar os dados de um indivíduo já cadastrado, primeiramente o usuário deverá informar qual registro a ser alterado ou excluído, fazer as alterações ou exclusão desejadas e então clicar no botão “Confirmar” para atualizar os dados ou confirmar a exclusão do registro.

4.4.2.2 – Implementação do Caso de Uso Autenticar Indivíduos

O caso de uso “Autenticar Indivíduos” é executado sempre que um indivíduo desejar que sua identidade seja autenticada. Para tanto, o usuário deve clicar no botão “Autenticar” disponível no Menu Principal do sistema para ter acesso esta funcionalidade.

Primeiramente o usuário informa a identificação por meio da digitação do código pessoal, em seguida apresenta uma das impressões digitais cadastras anteriormente para o código informado. Feito isto, basta clicar no botão “Autenticar” para que o sistema verifique a veracidade da informação. A figura 68 mostra a interface de autenticação.

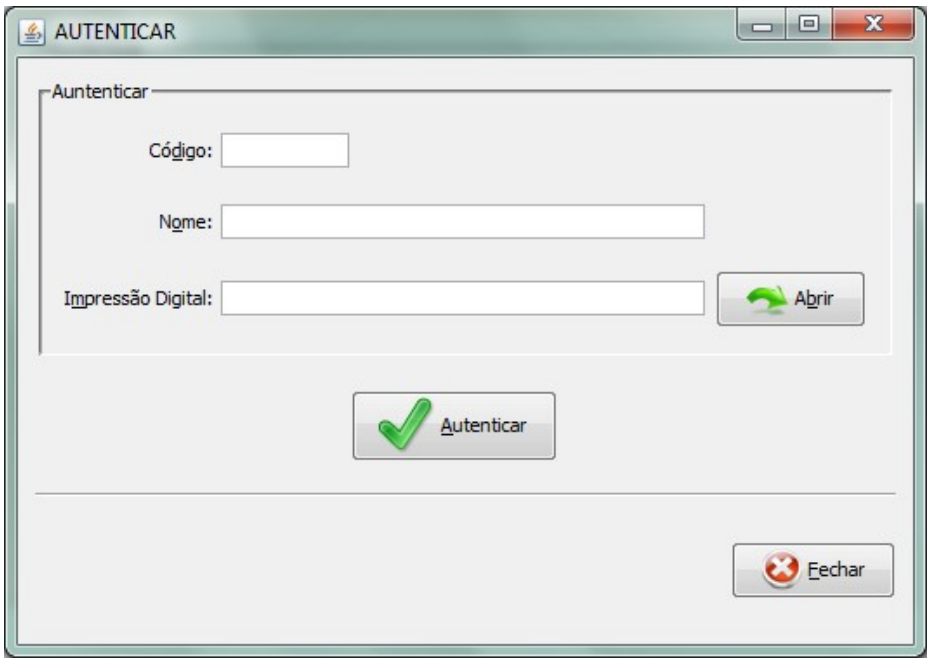

Figura 68 – Interface de autenticação

Se a identidade informada realmente estiver cadastrada, o sistema recupera o modelo biométrico armazenado para cada impressão digital que tenha sido apresentada na realização do cadastro da referida pessoa, comparando com o

modelo gerado a partir da impressão digital a ser autenticada. Uma mensagem é exibida ao usuário informando o resultado da autenticação ou informando que a identidade apresentada não está cadastrada.

4.4.2.3 – Implementação do Caso de Uso Identificar Indivíduos

O caso de uso “Identificar Indivíduos” é executado sempre que um indivíduo desejar que sua identidade seja definida a partir de uma impressão digital informada. O usuário acessa tal funcionalidade por meio do botão “Identificar” disponível no Menu Principal do sistema.

Para que a identidade seja estabelecida, o usuário necessita apenas apresentar a impressão digital a qual deseja ser identificada e clicar no botão “Identificar”. O sistema gera um modelo biométrico da impressão digital apresentada e procura uma que seja equivalente na base de dados. Uma mensagem é exibida com a identificação caso esta seja encontrada, caso contrário é exibida uma mensagem informando que a impressão digital apresentada não pertence a nenhum indivíduo cadastrado. A figura 69 mostra a interface de identificação.

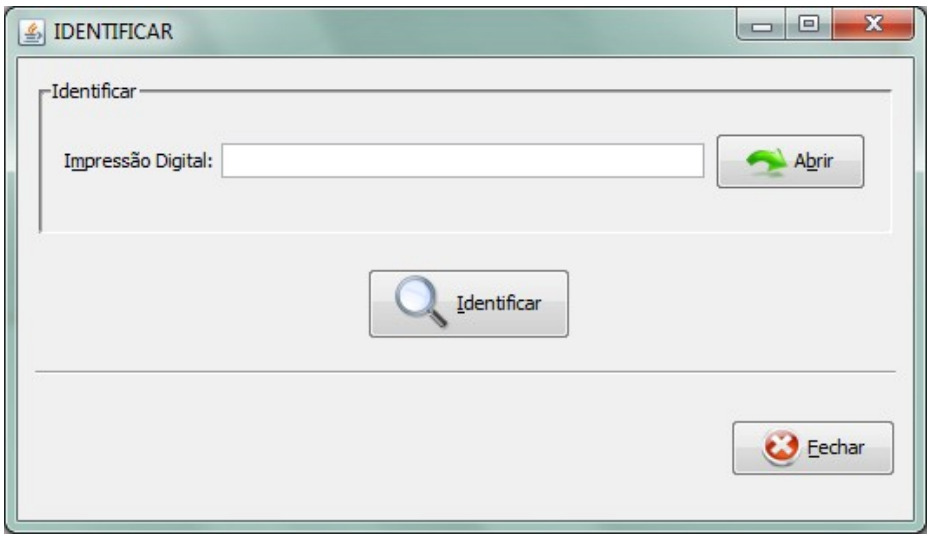

Figura 69 – Interface de identificação

5 – CONCLUSÃO

Neste capítulo serão feitas as conclusões obtidas no desenvolvimento do projeto. Também serão citadas algumas aplicações que podem ser desenvolvidas com os conhecimentos adquiridos, bem como dar continuidade no projeto aqui desenvolvido.

5.1 – CONSIDERAÇÕES FINAIS

O uso da biometria para a identificação de pessoas já é realidade sendo pouco provável que outro conceito a substitua. O constante avanço das tecnologias de comunicação faz com que haja cada vez mais interação entre as pessoas e aumente a utilização de serviços, principalmente os que estão ligados ao setor financeiro. Sendo assim, o desenvolvimento deste projeto se justifica diante da crescente demanda do mercado. Outro fator importante é o conhecimento adquirido das tecnologias envolvidas em biometria, que dá subsídios para que possa atuar profissionalmente em inúmeras áreas futuramente.

Mesmo que certas tecnologias se mostrem caras e de difícil implementação, elas não podem ser desprezadas na área de segurança, uma vez que o custo pode justificar sua necessidade. A combinação de várias tecnologias pode significar uma barreira praticamente intransponível se bem implementada. Além disso, a comodidade e facilidade de utilização do sistema por parte do usuário devem ser levadas em conta já que com a crescente demanda por processos de reconhecimento, a atenção que estes dispensam a senhas e outros métodos tende a diminuir.

A utilização de técnicas de processamento de imagens tem sido utilizada em diversos projetos comerciais de sucesso. Órgãos de segurança como FBI e NSA (*National Security Agency*) têm investido grandes somas em pesquisa e

desenvolvimento de tecnologias no intuito de estar sempre um passo à frente dos criminosos e usuários mal intencionados.

Uma das dificuldades encontradas foi o total desconhecimento da área que se optou por desenvolver nossa pesquisa, começando sempre pelos aspectos mais básicos até propostas mais elaboradas para a resolução do problema. A opção de dividir o projeto em duas partes foi satisfatória, pois com os conhecimentos adquiridos foi possível realizar a implementação do sistema biométrico, mesmo com a complexidade que o problema exige.

5.2 – TRABALHOS FUTUROS

A implementação de um sistema de autenticação e identificação por impressão digital que apresente todas as funcionalidades exigidas para sua adoção é um projeto futuro. Para tanto, os problemas não tratados na implementação deste trabalho como métodos mais eficientes para melhorar a qualidade das imagens e a invariância quanto à rotação ou translação tem que ser mais bem estudados.

Para o problema da qualidade das imagens é necessário o estudo de outros métodos de filtragem ou alguma outra forma de se obter a estrutura integra das imagens que se apresentam com falhas, pois assim estas podem ser utilizadas pelo sistema desenvolvido neste trabalho.

Uma possível solução para o problema de rotação e translação é estudar métodos para calcular a imagem direcional das imagens de impressão digital. A imagem direcional determina a orientação das cristas e vales que formam as impressões digitais, ou seja, os ângulos formados pelas riscas da imagem. Dessa forma é possível localizar um ponto de referência que seja único em toda a imagem, de modo que este possa ser utilizado no processo de localização das minúcias.

A imagem direcional pode ser utilizada também para classificar as impressões digitais entre as cinco classes apresentadas neste trabalho. Esta classificação pode ser utilizada no processo de identificação, quando o sistema biométrico busca uma

identidade na base de dados a partir da impressão digital apresentada, pois apenas as impressões de mesma classe seriam comparadas, o que tornaria o processo muito mais rápido e eficiente.

O objetivo futuramente é utilizar os conhecimentos adquiridos neste trabalho para o desenvolvimento desse aplicativo para dispositivos móveis.

REFERÊNCIAS

ALBUQUERQUE, Marcelo Pontes de, et al. **Análise de Imagens e Visão Computacional**, V Escola do CBPF, Rio de Janeiro, 2004.

ALVES, Filipe Ferreira. **Desenvolvimento de Aplicação Biométrica Para Reconhecimento de Impressão Digital Através de Um Dispositivo Móvel**. 2007. 62p. Monografia **–** Universidade Federal da Bahia, Salvador, 2007.

BIOLAB **– Biometric System Laboratory**. DEIS **–** University of Bologna. Disponível em: <http://biolab.csr.unibo.it/home.asp> Acesso em junho de 2010.

BR, foto.com. **Histograma - O que é?** Disponível em: <http://forum.brfoto.com.br/index.php?showtopic=58347&st=0>. Acesso em junho de 2010.

COSTA, Luciano; OBELHEIRO, Rafael; FRAGA, Joni. **Introdução à Biometria**. 2006. 49p. Universidade Federal de Santa Catarina. Apostila do Departamento de Automação de Sistema, Florianópolis, 2006.

COSTA, Luciano. **Um Modelo de Autenticação Biométrica para *Web Banking***. 2007. 100p. Dissertação (Mestrado) **–** Universidade Federal de Santa Catarina, Florianópolis, 2007.

COSTA, Silvia Maria Farani. **Classificação e Verificação de Impressões Digitais**. 2001. 123p. Dissertação (Mestrado) **–** Universidade de São Paulo, São Paulo, 2001.

DEKKER, Marcel. ***Pattern Recognition and Image Preprocessing*.** 2002. 711p. Northern Illinois University De Kalb, Illinois, Second Edition, 2002.

DESSIMOZ, Damien; RICHIARDI, Jonas. **Multimodal Biometrics for Identity Documents.** 2006. 161p. UNIL **–** Université de Lausanne, Lausanne, Suíça, 2006.

DETROIT, Unets. Disponível em: <http://unstructuredlibertynetworks.files.wordpress.com/2009/11/irisscan.jpg> Acesso em junho de 2010.

DIREITA, Rua. Disponível em: <http://www.ruadireita.com/info/img/camaras-de-vigilancia-prevencao-e-seguranca-ou-invasao-de-privacidade.jpg> Acesso em junho de 2010.

FARIA, Diego Resende. **Reconhecimento De Impressões Digitais com Baixo Custo Computacional Para Um Sistema De Controle De Acesso**. 2005. 100p. Dissertação (Mestrado) **–** Universidade Federal do Paraná, Curitiba, 2005.

G1.com, O Portal de Notícias da Globo. Disponível em: <http://g1.globo.com/Noticias/SaoPaulo/foto/0,,11260818-EX,00.jpg> Acesso em junho de 2010.

GARCIA, Rodrigo de Luis, et al. **Biometric Identification Systems**. 2003. 19p. Signal Processing, Elsevier, 2003.

GONZALES, Rafael C.; WOODS, Richard E. **Digital Image Processing**. University of Tennesse e Perceptics Corporation,1992.

GREGORY, Peter; SIMNO, Michael. **Biometrics for Dummies.** 2008. 306p. Wiley Publishing, Inc**.**, Indianapolis, Indiana, 2008.

HEALTH HAVEN, Forensic Medicine & Forensic Medicine Stock Photos at. Disponível em: <http://media-2.web.britannica.com/eb-media/43/102643-050-ABC1916.jpg> Acesso em junho de 2010.

HOUSE, Anna Builds a. Disponível em: <http://annabuildsahouse.files.wordpress.com/2009/11/fingerprint-lock-2.jpg> Acesso em junho de 2010.

JAIN, Anil; BOLLE, Ruud; PANKANTI, Sharath. **Biometrics Personal Identification in Networked Society.** 2002. 422p. Kluwer Academic Publishers, 2002.

JAIN, Anil; DUIN, Robert; MAO, Jianchang. **Statistical Pattern Recognition: A Review.** 2000. 34p. IEEE Transactions on Pattern Analysis and machine Intelligence, Vol. 22, 2000.

KENTUCKY, .gov. Disponível em: <http://techlines.ky.gov/NR/rdonlyres/2289B29F-EA3B-4C2C-96A9-D16BDF56C580/0/facial_rec.jpg> Acesso em junho de 2010.

MARION, André. **An Introduction to Image Processing**, Chapman and Hall, 1991.

MASCARENHAS, Nelson Delfino d'Ávila; VELASCO, F. R. D. **Processamento Digital de Imagens**. Ministério da Ciência e Tecnologia – MCT. Instituto de Pesquisa Espaciais – INPE, 1989.

MAZI, Renan Corio. **Identificação Biométrica Através da Impressão Digital Usando Redes Neurais Artificiais**. São José dos Campos: Instituto Tecnológico de Aeronáutica, 2009. 9p. Projeto de Iniciação Científica, 2009.

MORGAN, Jolvani. **Técnicas de Segmentação de Imagens na Geração de Programas para Máquinas de Comando Numérico**. 2008. 100p. Dissertação (Mestrado) – Universidade Federal de Santa Maria, Santa Maria, 2008.

OREGON, Inside. Disponível em: <http://insideoregon.uoregon.edu/wp-content/uploads/hand-300x284.jpg> Acesso em junho de 2010.

PACHECO, César Alexandre Rodrigues Anjos. **Autenticação com Impressão Digital**. Lisboa: Instituto Superior de Engenharia de Lisboa, 2003. 65p. Relatório submetido como requisito parcial para obtenção do grau de licenciado em Engenharia de Sistemas de Telecomunicações e Eletrônica, 2003.

PEREIRA, Leonardo de Pádua Costa. **Mapeamento de Imagens Binárias: Um Estudo Sobre Biometria da Mão**. 2003. 57p. Monografia – UNAMA: Universidade da Amazônia, Belém, 2003.

PRABHAKAR, Salil. **Fingerprint Classification and Matching Using a Filterbank.** 2001. 259p. Dissertação (Doutorado) **–** Michigan State University, East Lansing, Michigan, EUA, 2001.

PSYCHOLOGY, Encyclopedia. Disponível em: <http://psychology.jrank.org/article_images/psychology.jrank.org/pattern-recognition.3.jpg>. Acesso em junho de 2010.

ROVANI, André Zanin. **Sistema Para Captura Automática de Imagens de Íris**. 2006. 81p. Dissertação (Mestrado) **–** Universidade Tecnológica Federal do Paraná, Curitiba, 2006.

SEVERO, Carlos Emilio Padilha. **HSQLDB: um banco de dados livre escrito em Java**. 2008. 5p. GUJ **–** Grupo de Usuários Java, 2008.

TECHNOLOGIES, Maxcom. Disponível em: <http://syrianature.com/maxcom/images/STANDALONE_ACCESS_CONTROL_SYSTEM_11.JPG> Acesso em junho de 2010.

TRE/RO, Tribunal Regional Eleitoral de Rondônia. Disponível em: <http://www.tre-ro.gov.br/noticias/fotos/DSC01433.JPG> Acesso em junho de 2010.

JUNIOR, John Woodward; ORLANS, Nicholas; HIGGINS, Peter. **Biometrics.** 2003. 464p. McGraw-Hill/Osborne, New York, 2002.

ZONE, Pro Security. Disponível em: <http://www.prosecurityzone.com/Customisation/News/Images/3759-SignHear-7.jpg> Acesso em junho de 2010.