UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

FERNANDO TAMBERLINI ALVES

ESTUDO DE TÉCNICAS UTILIZADAS NO RECONHECIMENTO DE IDENTIDADE POR IMPRESSÕES DIGITAIS

RIO DE JANEIRO

2007

Fernando Tamberlini Alves

ESTUDO DE TÉCNICAS UTILIZADAS NO RECONHECIMENTO DE IDENTIDADE POR IMPRESSÕES DIGITAIS

Dissertação de Mestrado apresentada ao programa de pós-graduação do Núcleo de Computação Eletrônica - Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do título de Mestre em Informática.

Orientador: Antonio Carlos Gay Thomé

Rio de Janeiro
2007

CIP - Catalogação na Publicação

A474e

Alves, Fernando Tamberlini
Estudo de Técnicas Utilizadas no Reconhecimento de Identidade por Impressões Digitais / Fernando Tamberlini Alves. -- Rio de Janeiro, 2007.
248 f.

Orientador: Antonio Carlos Gay Thomé.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Programa de Pós-Graduação em informática, 2007.

1. Impressão Digital. 2. Biometria. 3. Autenticação. I. Thomé, Antonio Carlos Gay, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

FERNANDO TAMBERLINI ALVES

ESTUDO DE TÉCNICAS UTILIZADAS NO RECONHECIMENTO DE IDENTIDADE POR IMPRESSÕES DIGITAIS

Dissertação de Mestrado apresentada ao programa de pós-graduação do Núcleo de Computação Eletrônica – Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários a obtenção do título de Mestre em Informática.

Aprovado em 09 de março de 2007

Antonio Carlos Gay Thomé – Ph. D – IM/UFRJ

Ricardo Cordeiro de Farias – Ph. D – COPPE/UFRJ

Josefino Cabral Melo Lima – Ph. D – IM/UFRJ

Manuel Lóis Anido – Ph. D – IM/UFRJ

À minha mãe

AGRADECIMENTOS

À minha mãe pelo seu amor, carinho, dedicação e tudo mais. Ela sempre esteve ao meu lado durante a vida toda. Agradeço também às minhas irmãs e a minha sobrinha.

Ao professor Thomé por acreditar no meu trabalho até o último instante. Obrigado pelos seus conselhos, pela sua paciência e pela sua dedicação.

À minha namorada por seu carinho e companheirismo.

Aos amigos do Mestrado, do LABIC e do Laboratório de Projetos.

À CAPES pelo apoio financeiro.

RESUMO

ALVES, Fernando Tamberlini. **Estudo de Técnicas Utilizadas no Reconhecimento de Identidade por Impressões Digitais**. Rio de Janeiro, 2005. Dissertação (Mestrado em Informática) - Instituto de Matemática, Universidade Federal do Rio de Janeiro, 2007.

É perceptível a qualquer um a necessidade de se reconhecer a identidade de um indivíduo. Seja para proteger bens, para evitar riscos ou para garantir direitos. Sendo assim, a sociedade criou mecanismos que servem como meio de prova de identidade. Um documento de identidade, uma senha e o uso da impressão digital são exemplos destes mecanismos. Na demanda por meio de prova rápido, barato, eficiente e resistente a fraude emerge os sistemas automáticos de identificação por impressão digital (AFIS). Este trabalho consiste em um estudo das técnicas utilizadas nestes sistemas. Essas técnicas incluem as etapas de aquisição da impressão digital, do pré-processamento da imagem adquirida, da extração das características descritoras da imagem da impressão digital obtida, do reconhecimento e por fim da decisão. Como parte deste estudo, é implementado quatro métodos de extração de descritores e quatro métodos de verificação de impressão digital. Os métodos implementados são submetidos a uma base de testes comum e os resultados obtidos são comparados aos de outros trabalhos.

ABSTRACT

ALVES, Fernando Tamberlini. **Estudo de Técnicas Utilizadas no Reconhecimento de Identidade por Impressões Digitais**. Rio de Janeiro, 2005. Dissertação (Mestrado em Informática) - Instituto de Matemática, Universidade Federal do Rio de Janeiro, 2007.

Everyone knows the necessity of recognize the identity of the people. Either to protect goods, to prevent risks or to guarantee rights. Thus, the society created mechanisms that are able to ensure the identity. An ID, a password and the fingerprint are examples of these mechanisms. In the demand for a realible, robust, efficient and unfaked recognition way rise the Automatic Fingerprint Identification Systems (AFIS). This work consists of a study of the techniques used in these systems. These techniques includes the stages of fingerprint sensing, fingerprint analysis and representation, fingerprint recognition and decision. As part of this study, it is implemented four features extration methods and four fingerprint verification methods. The implemented methods are submitted to a common base of tests and its results are compared with other works.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AFIS	Sistemas Automáticos de Identificação de Impressões Digitais *Automatic Fingerprint Identification Systems*
CCD	*Charge Coupled Device*
CMOS	*Complementary Metal Oxide Semiconductor*
DPI	*Dot Pei Inch*
DNA	Ácido Desoxirribonucléico
FAR	Taxa de Falsa Aceitação *False Acceptance Rate*
FRR	Taxa de Falsa Rejeição *False Rejection Rate*
FVC	Competição de Sistemas de Verificação de Impressão Digital *Fingerprint Verification Competition*
gms	*Genuine Matching Scores*
ID	Impressão Digital
ims	*Impostor Matching Scores*
MCL	Matriz de Características Locais
NIST	*National Institute of Standards and Technology*
NGRA	Número de Reconhecimento Positivo ou Genuíno *Number of Genuine Recognition Attempst*

NIRA Número de Reconhecimento Negativo ou Impostor
Number of Impostor Recognition Attempst

PRIID Processo de Reconhecimento de Identidade por Impressão Digital

SB Sistema Biométrico

SUMÁRIO

1 INTRODUÇÃO

"Who am I? I'm Spider-man."

Peter Parker, *Spider-Man (Movie)*

1.1 Considerações Iniciais

Nos dias de hoje, poucas são as pessoas que não se surpreendem com a quantidade de documentos, de cartões e de senhas que possuem. Para evitar carteiras cheias ou memória sobrecarregada, elas buscam algum modo de diminuir essa grande quantidade. Utilizam o documento que contém maior número de informações, tentam concentrar vários serviços em apenas um cartão e quase sempre escolhem uma mesma senha. Tudo isso para minimizar o excesso. Mas se alguém indagar o motivo deste excesso a justificativa é rápida: é para comprovar que você é você. E se alguém perguntar o porquê dessa necessidade de comprovação de identidade a resposta é simples: é por questão de segurança.

No início do século XXI, o quesito segurança já justifica qualquer necessidade. Não importa a posição hierárquica que um governante ocupe ou o cargo que um empregado exerça ou o nível de instrução que a pessoa tenha. Todos considerariam o quesito segurança como algo básico e fundamental. A exigência de identificação protege o saldo bancário de um correntista, resguarda a intimidade individual e impede o acesso a uma área restrita. Portanto, por trás da expressão "é por questão de segurança" estão o direito a posse privada, o direito de privacidade e a proteção contra a ameaça potencial que qualquer um possa representar. Há também outras inúmeras razões, todavia as apresentadas já constituem motivos suficientes para iniciar o estudo de um processo automático de comprovação de identidade.

O ato de reconhecer identidade responde pelo menos uma das três seguintes perguntas: Quem é essa pessoa? Essa pessoa é quem ela diz ser? Essa é a pessoa procurada? Perguntas essas que são explicitamente ou implicitamente feitas em diversos momentos e inúmeras vezes. Cada uma destas perguntas possui um propósito e consome um determinado recurso. Porém o objetivo principal é alcançar a resposta, não deixando de avaliar seu custo e sua precisão.

Um filho não precisa provar para mãe que ele é o filho dela e um gerente de banco nem sempre exige a senha de um cliente. Mesmo não havendo uma ação formal de identificação, tanto a mãe quanto o gerente responderam uma das perguntas citadas acima. Num grupo pequeno de pessoas como uma família ou uma equipe de trabalho o reconhecimento é natural. Todavia, em um grande conjunto de pessoas a tarefa de reconhecer a identidade de alguém passa a ser difícil e crítica.

Algo precisaria ser concebido a fim de resolver esse problema crítico. A criação de um documento pessoal, a utilização de uma informação secreta e o uso de características físicas foram as soluções encontradas. Sendo assim, a unicidade de uma pessoa pode ser confirmada por três tipos de provas: a prova por posse, a prova por conhecimento e a prova por propriedade (SUCUPIRA, 2004). Em outras palavras, o indivíduo é reconhecido pelo que ele tem, pelo que ele sabe ou pelo que ele é. O cartão, a senha e a impressão digital (ID) são, respectivamente, exemplos dessas três provas. Contudo, não é verdadeiro afirmar que essas provas são infalíveis. Um cartão pode ser perdido, adulterado ou copiado. Uma senha pode ser descoberta, esquecida ou repassada. Uma característica biométrica pode ser mutável, pode não estar presente em todas as pessoas ou pode ser de difícil coleta. Ou seja, cada uma tem suas vantagens e desvantagens. A dificuldade reside na escolha do método de prova a ser usado.

Para avaliar um método de prova algumas métricas já foram propostas (OGORMAN, 2003). Mas o pensamento que permanece é que a prova por posse, a prova por conhecimento e a prova por propriedade não competem entre si, e sim se complementam. Segundo O'Gorman (2003, p.2038), "... a melhor solução de autenticação depende da aplicação em questão...". Apesar de não existir competição entre elas, a prova por propriedade surge como a prova que proporciona maior defesa contra a fraude. Esta faz uso da biometria, que neste contexto, significa o uso de características fisiológicas e comportamentais para reconhecer a identidade de uma pessoa. A assinatura, o DNA, a face, a

geometria das mãos, a impressão digital, o íris, o modo de andar, o modo de digitar, o odor, a orelha a voz são exemplos de características biométricas usadas para reconhecer identidade (HONG, 1998), (MALTONI et al., 2003) e (JAIN et al., 2004a).

É fácil perceber que - ao contrário de um cartão ou de uma senha - a impressão digital de um indivíduo não é perdida nem esquecida, que um assassino não nega quando sua impressão digital é encontrada na arma do crime e que o DNA é uma prova inquestionável na determinação de paternidade. A biometria é intrinsecamente um identificador natural. Mas é errado afirmar que por usar dados biométricos um sistema de identificação é infalível. Apesar de os sistemas biométricos estarem entre os mais modernos, eles não podem ser glorificados. Quesitos como a exatidão, a escala, a segurança e a privacidade foram propostos por Jain et al (2004a) para facilitar a análise de um sistema biométrico.

Como objeto deste estudo escolheu-se a impressão digital em função da facilidade de coleta, do histórico de utilização e a da sua popularidade - de acordo com Maltoni et al (2003), cerca de 52% dos sistemas biométricos do ano de 2002 são baseados em impressão digital - e outros motivos justificam essa opção. Mesmo existindo inúmeros produtos de *AFIS*[1] disponíveis no mercado, inúmeras pesquisas já realizadas sobre o tema e ser popularmente considerado um assunto bastante explorado, ainda existem muitos desafios a serem superados nesta área (PRABHAKAR, 2001), (ROSS, 2003) e (MALTONI et al., 2003). A falta de qualidade e distorções não lineares presentes nas imagens de ID, o crescente número de dispositivos de aquisição de baixo custo e não tão eficientes e o desempenho ainda não completamente satisfatório encontrado em cada uma das diversas etapas do processo ainda são problemas a se combater (ROSS, 2003). Conforme Maltoni et al (2003), os estudos que combinem várias técnicas de verificação ou identificação ainda carecem de pesquisa e de avaliação.

1.2 Reconhecimento de Identidade por Impressões Digitais

Reconhecer identidade é necessário. Se não fosse não haveria documentos de identidade, cartões magnéticos, senhas e outras coisas mais. A discussão que emerge é qual é o melhor meio de identificar. Essa escolha envolve o quanto se gasta e o desempenho do método, ou seja, o custo/benefício. Durante o ato de reconhecimento, implici-

[1]Esses sistemas são conhecidos como Sistemas Automáticos de Identificação de Impressões Digitais *(Do inglês AFIS - Automated Fingerprint Identification System).*

tamente ou explicitamente, o responsável pelo reconhecimento, chamado aqui de Identificador, faz uma ou algumas perguntas e o indivíduo a ser identificado, chamado aqui de Identificável, apresenta alguma coisa para provar a sua identidade. O esquema mostrado na Figura 1.1 ilustra o ato de reconhecimento.

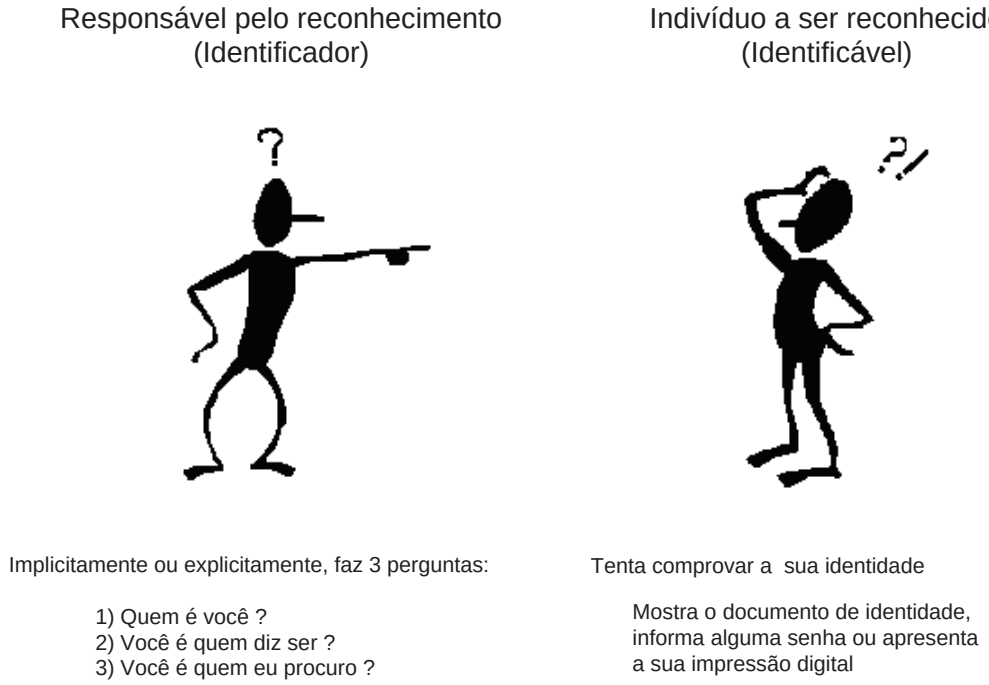


Figura 1.1: Processo de reconhecimento de identidade.

Afigura-se que as três perguntas tratam da mesma coisa e que portanto são sinônimas. No entanto, elas não são, há diferenças elas. Na primeira pergunta - Quem é essa pessoa? - o Identificador não conhece de antemão a identidade do Identificável. O Identificado se propõe a ser reconhecido, porém não dispôs de nenhuma prova prévia. Resta ao Identificador comparar a identidade do Identificável com as identidades já registradas. Já na segunda pergunta - Essa pessoa é quem ela diz ser? - o Identificador informa ao Identificável a sua identidade, a única tarefa do Identificador é verificar se o Identificável é quem diz ser. E na terceira pergunta ocorre algo diferente. Não existe a vontade formal do Identificável de ser reconhecido, ou seja, ele não oferece nenhuma prova de identidade ao Identificador. Cabe a este último investigar e procurar reconhecer a identidade do indivíduo em questão (JAIN et al., 2004a).

Com já mencionado, há inúmeras maneiras de se auferir a identidade de uma pessoa. Esses meios são classificados em três tipos principais: prova por posse, prova por

conhecimento e prova por propriedade (SUCUPIRA, 2004). Um tipo de prova não exclui e nem sobrepõe ao outro, cada um deles possuem vantagens e desvantagens. Eles não competem entre si, e sim se complementam. A Figura 1.2 esclarece o emprego desses tipos de prova. Existem situações nas quais duas provas são usadas simultaneamente, como por exemplo, no momento de um saque em um terminal bancário automático. O cliente insere seu cartão e logo em seguida informa a sua senha. Já em outras ocasiões basta o indivíduo apresentar sua carteira de motorista para confirmar sua identidade. A escolha de tipo de prova vai depender dos requisitos do sistema em questão. O custo, o grau de segurança, a facilidade de uso e outros mais são itens que servem de critério da escolha a ser feita.

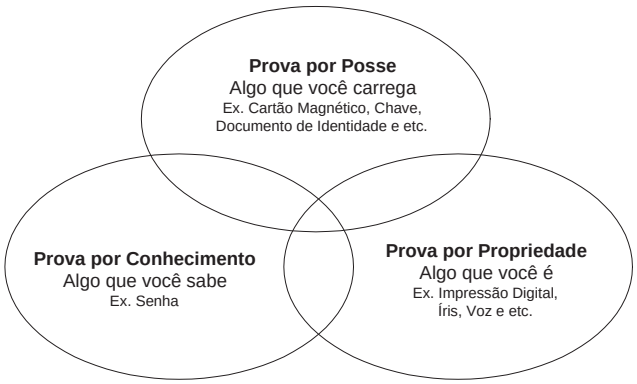


Figura 1.2: Tipo de provas usadas no reconhecimento de identidade.

1.3 Proposta

A proposta desta pesquisa é realizar um estudo sobre a metodologia e as diferentes técnicas computacionais empregadas no Processo de Reconhecimento de Identidade por Impressão Digital (PRIID). O esquema apresentado na Figura 1.3 ilustra as principais etapas que compõem um sistema de um PRIID. O estudo conduzido neste trabalho aborda todas as etapas do processo, porém se concentra nas etapas de representação e de reconhecimento.

- Etapa 1 - é onde ocorre a aquisição da imagem da impressão digital. Esta etapa se ocupa da forma (voluntária ou involuntária), do meio (on-line ou off-line), do modo (batida, rolada ou arrastada) na qual a ID é adquirida; se preocupa também com o

estado da ID e a qualidade da imagem obtida; e também com as especificações e tecnologia do dispositivo de aquisição.

- Etapa 2 - trata de como armazenar os dados obtidos, ou seja, o quê armazenar (a própria imagem ou as características extraídas) e como armazenar (criptografado ou não; indexado ou não), com vistas a proporcionar um bom desempenho nas buscas.

- Etapa 3 - O principal objetivo desta esta etapa é a extração de características identificadoras da ID. O produto final desta etapa é um vetor com informações a serem utilizadas na etapa seguinte. Dependendo das etapas anteriores, a tarefa de extração precisa ser precedida de algum processamento que melhore a qualidade da imagem. Algoritmos que aprimorem e segmentam a imagem da ID são normalmente utilizados, além de outros métodos de pré-processamento.

- Etapa 4 - Nesta etapa ocorre o reconhecimento propriamente dito. Realiza-se a comparação da ID de entrada com as ID de referência. Se a comparação é de uma ID de entrada com as ID de referência de várias pessoas (1:N) dá-se o nome de identificação, já se a comparação é de uma ID de entrada com uma ID de referência de uma única pessoa (1:1) dá-se o nome de verificação. Para diminuir o espaço de busca (número de ID de referência) na etapa de identificação, pode-se, anteriormente, realizar as subetapas de indexação ou classificação.

- Etapa 5 - Nesta etapa final o ocorre a definição dos parâmetros que decidem se o reconhecimento foi positivo ou negativo. Esses parâmetros variam de acordo com a rigidez requerida pela aplicação.

1.4 Motivação

Por existir inúmeros produtos comerciais capazes de reconhecer a identidade por impressão digital e por ser um assunto estudado há um longo tempo, tem-se a impressão de que o tema já está esgotado. Apesar dos primeiros trabalhos sobre sistemas automáticos de reconhecimento de identidade por ID datarem de 1960 (ROSS, 2003) e existirem produtos comerciais que anunciam altas taxas de acerto. A principal motivação que norteou a escolha deste tema é o fato dele ser um tema complexo, ainda existir desafios a atacar e o domínio da tecnologia empregada no processo está restrita a poucos

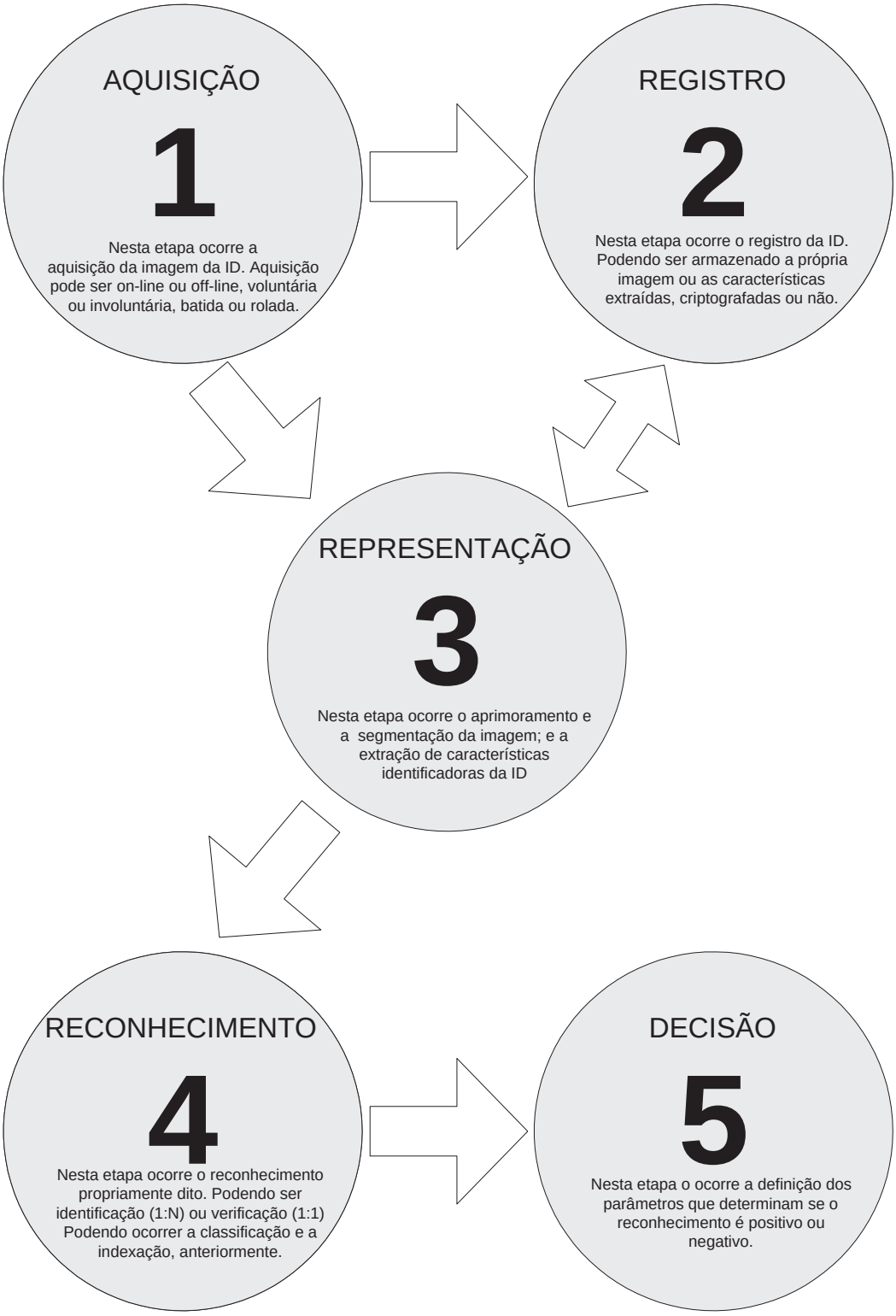


Figura 1.3: Etapas de um Processo de Reconhecimento de Identidade por Impressão Digital (PRIID).

grupos de pesquisa. Em sua tese de doutorado, Ross (2003) aponta cinco desafios a serem vencidos:

1. A nova geração de *scanners* do tipo *solid-state* está sendo cada vez mais usada. Este tipo de *scanner* quando embutido em outros tipos de sistemas tem seu tamanho muito reduzido. Este fato faz com que uma pequena área da ID seja adquirida que, no final, implica em um número reduzido de características identificadoras para serem extraídas. Portanto, surge a necessidade de criar estratégias mais robustas que sejam mais eficazes na localização das características e capazes de reconhecer mesmo quando há pouca informação disponível.

2. Devido ao avanço da tecnologia empregada nos sensores dos scanners, há hoje vários scanners com diferentes especificações. Todavia nem todos PRIID são compatíveis como todos os tipos de scanners existentes. A construção de um PRIID que independa do dispositivo de aquisição é um desafio ainda não superado.

3. O desempenho de um PRIID é afetado por distorções não lineares presentes em na imagem disponibilizada pelo leitor. Estas distorções aparecem em função do posicionamento e da pressão incorreta do dedo sobre o dispositivo de aquisição. Para aumentar o desempenho no PRIID, essas distorções devem ser reparadas pelo sistema.

4. É sabido que a ID quase não se altera com o tempo, entretanto podem ocorrer pequenos acidentes como cortes e queimadura que diminuem a confiabilidade do sistema. Tratar, prevenir ou remediar este problema é um desafio ainda em aberto.

5. Há ID que são intrinsecamente ruins, a extração de características é ineficaz e o desempenho do PRIID fica prejudicado. O desafio neste caso está na busca de estratégias para contornar o problema. Desta forma, o desempenho do PRIID fica muito prejudicado. Para isso, a utilização de sistemas multi-biométricos (aqueles que usam mais de um tipo de biometria) é uma solução a ser empregada para resolver este contratempo. Além disso, esses sistemas multi-biométricos possuem uma segurança maior.

1.5 Organização da Dissertação

Este trabalho possui cinco capítulos e seis apêndices cujos conteúdos são descritos a seguir.

O Capítulo 2 exibe uma visão geral sobre biometria, particularmente a impressão digital. Primeiramente apresenta a biometria como um todo, depois comenta seus tipos, suas vantagens e desvantagens, e por fim faz uma comparação entre elas. Depois é feita uma exposição sobre a impressão digital, sua história; sua formação e características; e no final é mostrado um estudo que garante a individualidade da ID.

O Capítulo 3 expõe o processo de reconhecimento de identidade por impressão digital (PRIID). Inicialmente aborda-se o processo de reconhecimento da identidade por completo. Na seqüência é feito um detalhamento de todas as etapas do PRIID. Começando pela aquisição e armazenagem da imagem da ID, passando pela representação que inclui técnicas de aprimoramento, segmentação e extração das características da imagem da ID, e no final as etapas de reconhecimento e decisão. No percorrer deste capítulo dá-se ênfase nas técnicas implementadas. No seu final é apresentado o protótipo desenvolvido.

O Capítulo 4 descreve algumas bases de imagens de ID disponíveis na quais os métodos estudados são aplicados. Bem como descreve o critério de avaliação adotado e comenta os resultados obtidos.

No Capítulo 5 faz-se um resumo sobre as técnicas estudadas e as dificuldades encontradas na realização desta pesquisa. Faz-se também uma projeção sobre trabalhos futuros.

No Apêndice A estão os resultados obtidos no processo de extração de características. No Apêndice C a E estão os testes relativos aos métodos de verificação implementados submetidos ao banco DB1 do FVC do ano de 2000. No Apêndice F estão os resultados do método de melhor desempenho submetido aos demais bancos da base de testes.

2 IMPRESSÃO DIGITAL

"Cada um que passa em nossa vida passa sozinho, porque cada pessoa é única, para nós, nenhuma substitui a outra."

Antoine de Saint-Exupéry

2.1 Biometria

No sentido literal, o vocábulo Biometria[1] significa medida da vida (MARQUES, 2004), como se pode concluir através do estudo etimológico da palavra biometria *(Biometria → do Grego bíos = vida + metr = r. de metrein, medir)*. Pode também significar o ramo da biologia que trata da análise estatística e quantitativa de medidas biológicas (WAYMAN et al., 2005). Contudo, o significado apropriado no contexto deste trabalho é aquele que define biometria como o uso de características fisiológicas e comportamentais para reconhecer a identidade de uma pessoa.

Restringindo-se à última acepção questiona-se o porquê de utilizar Biometria como forma de reconhecer identidade. Não existiria um modo mais fácil? A razão do uso de prova por propriedade, no caso por biometria, está relacionada com a demanda por um meio de identificar seguro, rápido, prático e resistente à fraude. Demanda esta atendida graças ao aparato computacional existente, sem o qual não seria possível. A seguir são descritas as qualidades que justificam o uso da biometria.

- Praticidade - Um dado biométrico[2] acompanha a pessoa onde ela estiver. Um indivíduo pode perder um documento de identidade, pode ter o cartão roubado ou esquecer uma senha facilmente. A possibilidade de um indivíduo deixar de ter um dado biométrico é bem menor do que nos casos anteriores.

[1] O mesmo que Biométrica. Já a palavra Antropometria é restrita às medidas do corpo humano.

[2] Biometria, dado biométrico e informação biométrica são considerados como sinônimos neste trabalho.

- Segurança - A possibilidade de falsificar um dado biométrico é praticamente nula, o que não acontece em relação às provas por conhecimento e por posse. Um documento de identidade pode ser falsificado e um programa invasor pode descobrir senhas facilmente. Por ser uma informação não trivial, a chance de fraude é próxima de zero.

Por essas e outras qualidades a biometria passou - e passa - a ser utilizada cada vez mais. Como forma de autenticação de sistemas, como meio de identificar criminosos em processos penais, como mecanismos de segurança de documentos e etc.

Literalmente, qualquer medida ou característica do corpo humano poderia ser usada como biometria desde que ela fosse capaz de reconhecer um indivíduo. Entretanto, a prática restringe esta qualquer medida e afirma que para uma informação biométrica estar apta a ser usada para reconhecer identidade deve seguir sete critérios (MALTONI et al., 2003), a saber:

- Universalidade - A maioria dos indivíduos deve possuir a biometria indicada;
- Unicidade - O dado biométrico deve ser capaz de distinguir o indivíduo;
- Imutabilidade ou permanência - O dado biométrico deve permanecer invariável ao longo do tempo;
- Desempenho - O processo de reconhecimento que utiliza determinada biometria deve ser computacionalmente rápido e consumir pouco recurso;
- Propensão à fraude - O processo de reconhecimento deve ser resistente a fraude;
- Aceitabilidade - O dado biométrico não deve ser invasivo sendo aceito pela população em questão;
- Facilidade de Coleta - O dado biométrico deve ser de fácil obtenção.

Em outras palavras, é pretendido que a biometria possua a mais alta eficácia possível a cerca desses sete critérios.

Atendido esses critérios, a medida ou característica pode ser utilizada como biometria. Predomina o conceito que os dados biométricos são subdivididos em duas

principais categorias: biometria fisiológica e biometria comportamental. A primeira categoria diz respeito a algo inato e intrínseco ao indivíduo, enquanto a segunda é o comportamento de uma ação que a pessoa pratica. Vale ressaltar que esta segunda categoria também é dependente de peculiaridades inatas da pessoa. São exemplos de biometria fisiológica: DNA, Face, Geometria da Mão, Impressão Digital, Íris, Odor, Orelha, Retina. Já a Assinatura, Modo de Andar, Modo de Digitar, Voz são exemplos de biometrias comportamentais (HONG, 1998), (MALTONI et al., 2003) e (JAIN et al., 2004a).

É perceptível que os dados biométricos comportamentais são mais suscetíveis a mudanças, o que não é uma qualidade desejada para uma biometria. Por essa razão, O'GORMAN (2002) se preocupou em propor uma nova nomenclatura para classificar os dados biométricos. Neste trabalho as biometrias são classificadas como estáveis *(stable)* ou instáveis *(alterable)*. Na primeira classe estão as biometrias com relativa constância e imutáveis e a segunda estão as biometrias que derivam de uma biometria estável, porém há um componente variável. Em estudos mais recentes apareceu uma nova categoria, a biometria química (CHIKKERUR, 2005). A medição do odor e a análise química do suor são exemplos desta nova categoria, mas ainda são poucos difundidos.

2.1.1 Tipos de Biometria

Na Figura 2.1 são ilustradas as biometrias fisiológicas mais estudadas, a saber: Arcada Dentária, Desenho das Veias, DNA, Face, Face 3D, Geometria da Mão, Impressão Digital, Impressão da Palma da Mão, Íris e Retina, Orelha, Termograma Facial, Termograma da Mão. E na Figura 2.2 estão as biometrias comportamentais: Assinatura, Modo de Andar, Modo de Digitar e Voz. A seguir é feito breve comentário sobre esses exemplos de biometria.

- Arcada Dentária

Não é uma biometria a ser utilizada em sistemas automáticos de autenticação, pois é de difícil coleta e possui baixo grau de unicidade e de permanência. Entretanto, é muito empregada no reconhecimento de cadáver. Isto deve ao fato de ser a estrutura mais resistente do corpo, capaz de resistir à carbonização em temperaturas de até 800^{o}C e por ser o local onde o material genético fica preservado por mais tempo.

A identificação de um cadáver pela arcada dentária se realiza através da comparação entre as chapas de raios-X feitas pelo cirurgião-dentista do suposto falecido e

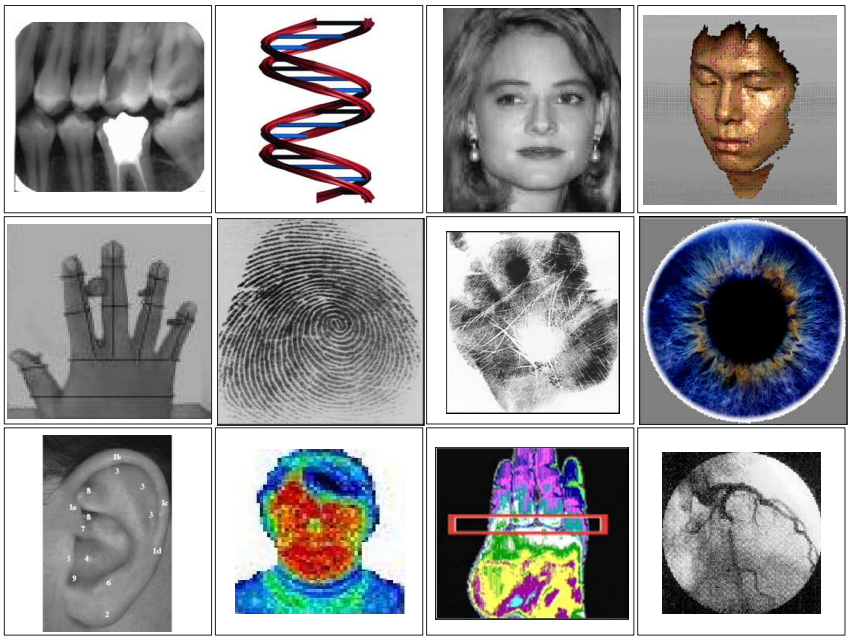


Figura 2.1: Tipos de biometria fisiológica: arcada dentária, DNA, face, face3D, geometria da mão, impressão da palma da mão, impressão digital, íris, orelha, termograma facial, termograma das mãos e desenho das veias.

chapas dos dentes tiradas do cadáver exatamente do mesmo ângulo. Depois essas imagens são sobrepostas para se aferir as semelhanças do formato dos dentes e de eventuais trabalhos odontológicos, como restaurações, canais, coroas e próteses. De uma maneira geral, qualquer informação na ficha odontológica da pessoa pode ajudar nessa comparação, principalmente irregularidades como dentes tortos, encavalados ou espaçados.

O reconhecimento de cadáver pela arcada dentária possui confiabilidade, sendo aceita como método de prova em instituições forenses. Conforme ratifica o médico forense Malthus Fonseca Galvão, do Laboratório de Antropologia Forense do Instituto Médico Legal de Brasília: "Consideramos a identificação pela arcada dentária tão confiável quanto a feita pelo DNA"(FOÇAGA, 2002, p. 37).

- Desenho das Veias

O desenho das veias, principalmente o desenho das veias nas mãos, propicia um dado biométrico robusto que pode ser usado em um sistema biométrico de identificação (NEWHAN, 1995 apud HONG, 1998). A imagem das veias das mãos pode ser facilmente obtida a partir de uma câmera infravermelha. O desenho das veias não pode ser modificado por cirurgias, o que o torna resistente às ações do próprio indivíduo. Em

outras palavras, o portador não consegue alterar ou diminuir a qualidade deste dado biométrico. Contudo, esta biometria não possui permanência satisfatória, mudando com o avanço da idade. Pesa contra esta biometria, o fato de ser um dado que precisa de um dispositivo de aquisição de grande tamanho físico e que os sistemas biométricos baseados no Desenho das Veias ainda não se mostraram capazes de atingir alto desempenho no processo de reconhecimento de identidade (HONG, 1998).

- DNA

O Ácido Desoxirribonucléico (DNA)[3] é uma molécula. Entretanto, assim como a arcada dentária, o reconhecimento de identidade pelo DNA se diferencia das demais por não ser um processo automático e por não ser usado em sistemas de autenticação. Isto é justificado por ser um processo invasivo, complexo e por envolver questões éticas. Desta forma, o uso do DNA se restringe ao processo de investigação forense, como por exemplo, o reconhecimento de paternidade.

- Face e Face 3D

Indubitavelmente, é pela face que a maioria das pessoas reconhece a identidade de outro, exceto para aqueles portadores de deficiência visual. O reconhecimento da face é um campo de pesquisa bastante aquecido e fértil, incluído trabalhos de detecção de face, de reconhecimento a partir de imagem estática da face em ambiente controlado e de reconhecimento da face através de imagem dinâmica em ambiente não controlado. Entende-se por ambiente controlado aquele que possui suas propriedades essencialmente constantes. Ou seja, à distância e a posição entre a câmera e a face, a iluminação, o ambiente de fundo, os dispositivos de aquisição e entre outras propriedades mantidas praticamente imutáveis. Já no ambiente não controlado ocorre o oposto. Por ter uma forma de aquisição não invasivo e de logo alcance, o reconhecimento de face surge como um método no qual não há necessidade de colaboração do indivíduo a ser reconhecido. Uma qualidade difícil de ser encontrada em outros meios de identificação.

Além destes atributos favoráveis, a grande aceitabilidade perante a sociedade torna o uso da face como dado biométrico o modo mais amigável de reconhecimento de identidade (ATICK et al, 1998; NEWHAM, 1995; TURK & PENTLAND, 1991 apud HONG, 1998). Foi no início da década de 70 que surgiram os primeiros trabalhos de

[3]Sigla na língua inglesa de *Deoxyribonucleic acid*, ADN na língua portuguesa.

reconhecimento de faces. Eles eram baseados principalmente nas medidas de partes da face como olhos, sobrancelhas, nariz, lábios, forma do queixo e etc. (CHELLAPA et al, 1995 apud HONG, 1998). Não obstante, os estudos sobre o reconhecimento de face ficaram por um tempo esquecidos devido à ausência de recursos computacionais e de algoritmos de extração de características razoáveis (CHELLAPA et al, 1995 apud HONG, 1998), sendo retomados somente no final dos anos 80.

Desde então, em complemento os métodos baseados na extração de atributos da face surgiram outras abordagem como: *principle component analysis (PCA)* (TURK & PENTLAND, 1991 apud HONG, 1998); *linear discriminant analysis (LDA)* (SWETS & WENG, 1999 apud HONG, 1998); *singular value decomposition (SVD)* (HONG, 1991 apud HONG, 1998); análise de características locais (ATICK et al, 1998 apud HONG, 1998) e técnicas que usam redes neurais (VALENTIN et al, 1994 apud HONG, 1998). Apesar dessas várias abordagens, Moutinho (2005) argumenta que os trabalhos de reconhecimento de face podem ser classificados em dois grupos: os baseados nas medidas de características faciais e os baseados na informação da própria imagem.

Em sua tese, HONG (1998) enumera as fases de um sistema de reconhecimento de faces como: *(i)* detectar se existe face ou não na imagem adquirida; *(ii)* localizar a face se existir e *(iii)* reconhecer a face. Por fim, pelo desempenho limitado pela dependência das condições de luz, pose e da expressão facial que as imagens de duas dimensões possuem, emerge os sistemas baseados em face 3D. Estes modelos de face 3D são construídos através da captura de imagens a partir de diferentes pontos de visão, obtendo assim mais informações as imagens 2D e por conseqüência tornando-os mais robustos (LU et al., 2004a) e (LU et al., 2004b).

- Geometria da Mão

A mão possui diversas características físicas que oferecem inúmeros dados e medidas suficientes para serem utilizadas como biometria. O comprimento e a largura dos dedos, a forma da mão e a espessura da palma são exemplos destes dados disponíveis. Existem mais de 4.000 sistemas biométricos baseados na Geometria da Mão instalados no mundo (DIECKMANN et al., 1997 & NEWHAN, 1995 apud HONG, 1998). A Geometria da Mão é uma biometria de fácil coleta e de simples processamento. O método de extração de características é simples, não necessita de dispositivos de aquisição com grande sensibilidade e é indiferente aos ruídos presente na biometria. Entretanto, não

possui boa distingüibilidade, sendo especialmente utilizada para sistemas de verificação e não para identificação (JAIN et al., 2004a). Não existem muitos trabalhos na literatura científica que empregam este dado biométrico (JAIN et al., 2004a). Sidlauskas (1988, apud JAIN et al, 1999c) apresenta um dispositivo que trabalha com a imagem 3D da mão, por conseguinte obtém mais dados. Outras questões que prejudicam o emprego desta da geometria da mão são o fato de exigir equipamento com uma área de captura grande e também o processo ser de fácil fraude.

- Impressão da Palma da Mão

A palma da mão possui a mesma estrutura de pele presente na impressão digital e, portanto, pode servir como uma biometria. Entretanto, poucos estudos foram feitos sobre o uso da impressão da palma da mão como informação biométrica (DUTA et al., 2002). Além das cristas e dos vales das papilas, os padrões das linhas da mão podem ser utilizados como características que identificam o indivíduo. Na medicina, as informações contidas na palma da mão também servem como indicadores de anomalias médicas como síndrome de DOWN e outras desordens genéticas (DUTA et al., 2002).

Em seu trabalho, Duta el at. (2002) investiga a viabilidade de um método de verificação baseado em impressão da palma da mão. Ele apresenta um método de extração de características e de comparação e afirma que a impressão da palma da mão possui um grande poder discriminatório. Por fim, baseado nos seus resultados, ele indica que esta biometria pode ser utilizada para melhorar os sistemas biométricos baseados em ID, nos quais as impressões digitais não podem ser obtidas corretamente.

- Impressão Digital

É descrita na segunda seção deste capítulo.

- Íris

Íris é uma membrana arredondada retrátil e diversamente pigmentada. É a coroa circular colorida do olho humano que atua sobre a pupila, por conseqüência controla a quantidade de luz que entra nos olhos. O padrão da pigmentação contido na íris é determinado por processos morfogenéticos caóticos presentes na fase embrionária do indivíduo, ela é única para cada pessoa e para cada olho, e permanece igual durante a vida toda (HONG, 1998), (DAUGMAN, 1999a apud MALTONI et al., 2003). Por ficar protegida do ambiente externo pelas pálpebras e por não ser passível de modificações cirúrgicas

(DAUGMAN, 1993 apud HONG, 1998), fica resguardada a sua qualidade, permanência e universalidade. Não obstante, é de difícil coleta. O processo de aquisição da imagem da íris não é uma operação trivial e precisa da cooperação do indivíduo. Passado isso, acredita-se que o reconhecimento de identidade pela íris é um modo rápido e acurado, prometendo um grande emprego desta biometria no futuro(MALTONI et al., 2003).

- Orelha

É a parte externa cartilaginosa do aparelho auditivo. Chega a ser inusitado a orelha ser utilizada como informação biométrica, no entanto existem trabalhos que mostram que as curvas do interior da orelha e outras medidas são capazes de distinguir uma pessoa. No trabalho Burge & Burger (2000) há uma exposição de sua viabilidade do seu uso como biometria. Desde 1949, já existem trabalhos que usam a orelha como biometria, como por exemplo, o proposto por Iannarelli (1989 apud BURGE & BURGER, 200) que consiste em uma técnica antropométrica de identificação baseado em 12 medidas extraídas da orelha. Conta a seu favor o fato de ser um exemplo de biometria passiva (BURGE & BURGER, 2000), ou seja, não há contato entre o indivíduo e o dispositivo de aquisição.

- Retina

O desenho formado pelos vasos sanguíneos presentes na retina é supostamente uma característica individual. A retina está situada no interior do globo ocular, esta localização torna-a de difícil acesso, por conseguinte, o processo de varredura da retina é um trabalho árduo e inconveniente para o indivíduo. Este fato justifica a pouca aceitação deste dado biométrico. Por outro lado, por ser pouco provável sua alteração ou replicação a torna uma das técnicas biométricas mais seguras (HONG, 1998). A baixa imutabilidade é também um ponto desfavorável.

- Termograma Facial e da Mão

"O sistema vascular subjacente à face humana produz uma assinatura facial única quando o calor passa pelo tecido facial e é emitido através da pele" (TRS, 1998 apud HONG, 1998, p. 14). Não somente a imagem do termograma facial, mas também o termograma da mão serve como um dado biométrico. A imagem do termograma é obtida por meio de câmeras infravermelhas. Assim como a face humana, o termograma facial é um método não invasivo, podendo assim se verificar a identidade sem a necessidade de contato e de cooperação do indivíduo. Ao contrário da imagem da face, o termograma

não é afetado pela iluminação do ambiente. Mas, o estado psicológico e físico da pessoa, como por exemplo, a temperatura do corpo e estado emocional, são fatores interferem no termograma. Acredita-se que esta biometria possua um poder discriminativo, mas ainda não foi provada a que grau.

Figura 2.2: Tipos de biometria comportamental: assinatura, modo de andar, modo de digitar e voz.

- Assinatura

Cada indivíduo possui o seu modo particular de assinar o seu nome. As formas das letras, a posição do ponto inicial da assinatura, a pressão da caneta são características perceptíveis suficientes para se verificar a identidade. É de fácil coleta e de grande aceitação. A sociedade aceita o uso de assinatura como meio de confirmar a identidade, o que é provado pela a exigência da assinatura em qualquer negócio jurídico (Ex. Cheques, Contratos, Documentos Judiciais etc). Há dois paradigmas no processo de reconhecimento por assinatura: o estático e o dinâmico (HONG, 1998). O primeiro avalia as características geométricas (forma e pressão da escrita) e o segundo leva em conta tanto essas características geométricas quanto a aceleração, velocidade e a trajetória da assinatura. Os sistemas biométricos que utilizam a assinatura como dado biométrico possuem acurácia razoável. Segundo Newhan (1995 apud HONG, 1998), aplicativos comerciais alcançam taxa de falso positivo de $0,58\%$ e taxa de falso negativo igual $2,1\%$. Todavia, é comum as pessoas apresentarem uma alta variedade de suas assinaturas o que dificulta o desempenho alto de sistemas biométricos baseados na assinatura.

- Modo de Andar

A maneira peculiar com que uma pessoa caminha pode ser utilizada como biometria. Não é esperado que o modo de andar seja uma biometria com alta unicidade, mas pode ser distinguível o suficiente para ser aplicada em um sistema de verificação de baixo nível de segurança (MALTONI et al., 2003). Fatores como idade, peso ou outras

desordens podem influenciar o andar de um indivíduo, prejudicando a sua permanência. Conta a seu favor a facilidade de obtenção e a não interação indivíduo em questão.

- Modo de Digitar

É o processo seqüencial de pressionar teclas de um teclado de computador. É a medição do intervalo de tempo entre a digitação de cada tecla. É esperado que esta biometria não possua boa unicidade e imutabilidade. Mesmo assim, é um método não intrusivo capaz de verificar a identidade de um indivíduo, ou seja, o modo de digitar pode ser monitorado sem que a pessoa saiba.

- Voz

A voz humana é gerada pela vibração do ar que é expulso dos pulmões pelo diafragma. As características da voz são determinadas pelas cordas vocais, lábios, boca e língua do indivíduo falante (CAMPBELL, 1997; NEWHAM, 1997 apud HONG, 1998). Outros fatores intermitentes como o estado de saúde e humor também modificam a voz (MARQUES, 2004). Por ser uma ação de uma pessoa é considerada como uma biometria comportamental, apesar de ser fortemente definida por características fisiológicas.

Distingüi-se o reconhecimento automático de voz do reconhecimento automático do locutor. O primeiro objetiva determinar o discurso do locutor, enquanto o segundo visa reconhecer a identidade do locutor. Considerando como uma informação biológica, restringe-se a sua aplicação ao reconhecimento de identidade. O reconhecimento pode ser através do uso de um texto determinado ou não. No caso de texto determinado o locutor fala uma frase de uma palavra. Já no texto não determinado o reconhecimento é baseado em uma frase qualquer do locutor, portanto um método mais difícil.

Intensos estudos a respeito do reconhecimento de voz/locutor vêm sendo realizados por diversos pesquisadores e centros de pesquisa mundo afora e diversos produtos comerciais no mercado (HONG, 1998). É uma biometria com boa aceitabilidade. Contudo, a voz humana não possui uma boa unicidade a fim de permitir a identificação a partir de uma grande base de dados, sendo praticamente usada para verificação, o que é explicado pelo fato de ser um dado biométrico suscetível a mudanças triviais como as condições físicas e emocionais do falante.

As biometrias acima mencionadas não esgotam o universo de tipos de biometria existentes, sendo apenas as mais em evidência. O trabalho de WAYMAN et al (2005)

discorre com maior profundidade sobre o assunto biometria.

2.1.2 Aspectos Comparativos

2.1.2.1 Em relação ao tipo de biometria

A seção anterior descreveu as peculiaridades de cada biometria, contudo as considerações apresentadas são insuficientes para avaliar qual dado biométrico deve ser usado em um determinado Sistema Biométrico. Para fundamentar essa escolha algumas questões devem ser analisadas. Os sete critérios já discutidos podem servir de medidas para esta análise. A Tabela 2.1 ilustra o grau (Baixo, Médio e Alto) desses sete critérios para cada biometria (MALTONI et al., 2003). Outros aspectos precisam ser examinados antes dessa escolha, a seguir são listadas algumas indagações a serem respondidas durante o processo de escolha de uma determinada biometria a ser empregada em um sistema biométrico.

- Qual é o modo de operação do Sistema Biométrico?
- Qual é o nível de exigência do Sistema Biométrico?
- Qual é a quantidade de usuários do Sistema Biométrico?
- Qual é o perfil do usuário do Sistema Biométrico?
- Há outro modo de prova concomitante?

Ao responder estas questões torna-se conhecido os requisitos e o contexto da aplicação a ser concebida, a partir daí consegue-se estabelecer os componentes do sistema biométrico. Ou seja, esclarecem-se os itens do sistema, como: a biometria empregada, a configuração do dispositivo de aquisição, o nível de rigor do sistema, os recursos computacionais necessários, o treinamento exigido e etc.

Por exemplo, se o modo de operação é de identificação já restringe o uso de alguns tipos de biometria, como a voz e a geometria da mão; se o nível de exigência é alto faz com que o processamento seja mais intenso o que acarreta em maior tempo de execução, e por conseqüência, exige mais recursos computacionais; se a quantidade de usuários é grande gera aumento de recursos de armazenamento e uma biometria com maior unicidade; pelo perfil do usuário se conhece qual biometria teria maior aceitação e se está presente em grande parte dessa população. Outro aspecto a considerar é se usuário

Tabela 2.1: Comparação entre os tipos de biometria (MALTONI et al., 2003).

DADO BIOMÉTRICO	UNIVERSALIDADE	UNICIDADE	IMUTABILIDADE	FACILIDADE DE COLETA	DESEMPENHO	ACEITABILIDADE	PROPENSÃO A FRAUDE
ASSINATURA	BAIXA	BAIXA	BAIXA	ALTA	BAIXA	ALTA	ALTA
DNA	ALTA	ALTA	ALTA	BAIXA	ALTA	BAIXA	BAIXA
FACE	ALTA	BAIXA	MÉDIA	ALTA	BAIXA	ALTA	ALTA
GEOMETRIA DAS MÃOS	MÉDIA	MÉDIA	MÉDIA	ALTA	MÉDIA	MÉDIA	MÉDIA
IMPRESSÃO DIGITAL	MÉDIA	ALTA	ALTA	MÉDIA	ALTA	MÉDIA	MÉDIA
ÍRIS	ALTA	ALTA	ALTA	MÉDIA	ALTA	BAIXA	BAIXA
MODE DE ANDAR	MÉDIA	BAIXA	BAIXA	ALTA	BAIXA	ALTA	BAIXA
MODO DE DIGITAR	BAIXA	BAIXA	BAIXA	MÉDIA	BAIXA	MÉDIA	MÉDIA
ODOR	ALTA	ALTA	ALTA	BAIXA	BAIXA	MÉDIA	ALTA
ORELHA	MÉDIA	MÉDIA	ALTA	MÉDIA	MÉDIA	ALTA	MÉDIA
RETINA	ALTA	ALTA	MÉDIA	BAIXA	ALTA	BAIXA	BAIXA
TERMOGRAMA DAS VEIAS DA MÃO	MÉDIA	MÉDIA	MÉDIA	MÉDIA	MÉDIA	MÉDIA	BAIXA
TERMOGRAMA FACIAL	ALTA	ALTA	BAIXA	ALTA	MÉDIA	ALTA	BAIXA
VOZ	MÉDIA	BAIXA	BAIXA	MÉDIA	BAIXA	ALTA	ALTA

pode complementar com uma senha ou um cartão o que aumenta o grau de segurança. Sendo assim, conclui-se que os sistemas a serem concebidos dependem do ambiente em questão.

Mesmo existindo mais de uma dezena de tipos de biometria, quatro delas se destacam: face, ID, íris e voz. A Tabela 2.2 mostra as vantagens e desvantagens de cada uma dela.

2.1.2.2 Em relação ao modo de prova

Após o alarde do uso da biometria como prova de identidade, veio a falsa idéia que essas técnicas que empregam biometria seriam infalíveis. No entanto, percebeu-se que a prova por propriedade também possui suas desvantagens. Com a preocupação de comparar os métodos de prova (prova por conhecimento, prova por posse e prova por propriedade), O'Gorman (2003) estabeleceu 6 (seis) métricas de avaliação: universo de busca, entropia, segurança *(Host-side security)*, protocolo de autenticação, conveniência e custo. Bem como as respostas de cada modo de prova à ataques específicos. Na conclusão

Tabela 2.2: Vantagens e desvantagens da Face, ID, Íris e Voz.

	VANTAGENS	DESVANTAGENS
FACE	- Não invasivo; - De fácil conferência pelo homem; - Dispositivo de aquisição usual (câmera); - Fotos Disponíveis em registros de ; identificação civil	-Facilmente alterado pelo cabelo, óculos, chapéus e etc; - Sensível a mudanças de pose, de expressão e de luz; - Faces mudam com o passar do tempo;
IMPRESSÃO DIGITAL	- Grande aceitação; - Facilidade de Uso; - Imagens de ID disponíveis em registros de identificação civil;	- A idade e a ocupação do indivíduo podem afetar a qualidade da ID; - A obtenção da impressão digital rolada requere treinamento e um dispositivo de aquisição robusto;
ÍRIS	- Não requer contato; - Órgão interno, portanto com maior proteção à agentes externos; - Não pode ser verificado pelo homem; - Requer alto treinamento;	- Invasivo e de difícil coleta; - Facilmente obscurecido pelas pálpebras, cílios, lentes, reflexos e etc;
VOZ	- Não invasivo; - Grande Aceitação; - Dispositivo de aquisição usual (microfone);	- Passível a alterações externas; - Não suficientemente distinguidor;

do seu trabalho, O'Gorman (2003) tece alguns comentários sobre os três tipos de prova, eles são apresentados a seguir.

A prova por conhecimento - como, por exemplo, o uso de senha - é um meio de prova conveniente, barata e eficaz. Entretanto, a necessidade do uso de várias senhas faz que os usuários escolham senhas fáceis ou senhas com alguma semântica, chegando a casos que o usuário não consegue memorizá-las e acabam escrevendo-as. Assim, as senhas podem ser roubadas ou mesmo ficam suscetíveis a "ataque dicionário" *(dictionary search attacks)*. Já a prova por posse tem a seu favor a questão de não ser de fácil reprodução, dando mais certeza ao processo de reconhecimento. Contudo, pode ser emprestado ou roubado, e tem um custo superior a prova por conhecimento. A prova por propriedade possui a particularidade de ser de difícil empréstimo e cópia. Vale ressaltar que O'Gorman salienta que informações biométricas estáveis *(stable)* são passíveis de cópias. Por fim, é ressaltado que cada meio de prova possui pontos favoráveis e desfavoráveis. O uso de um meio não exclui o outro, ele podem ser empregados concomitantemente. As

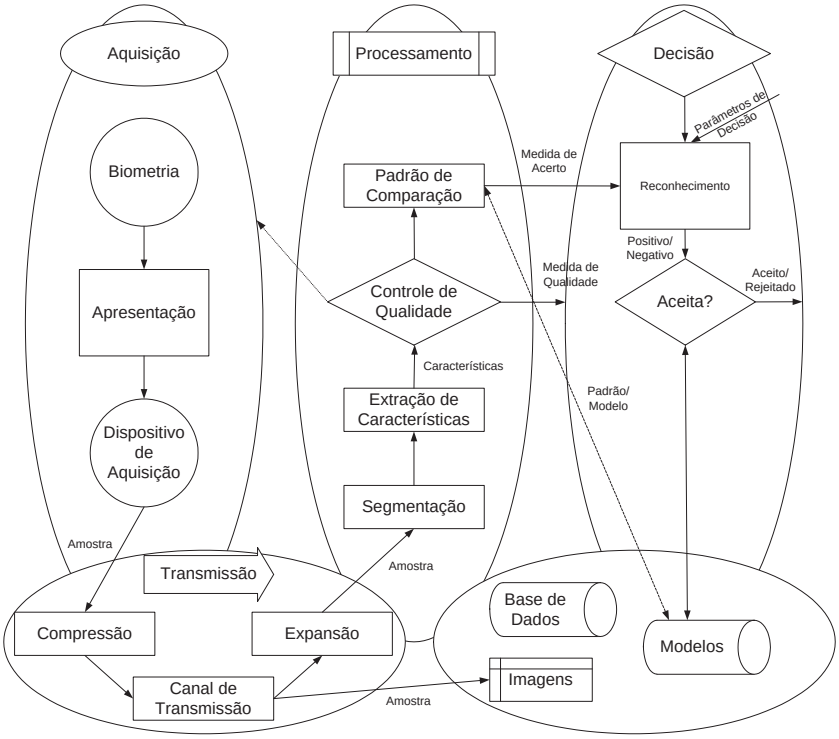


Figura 2.3: Sistema biométrico genérico (WAYMAN et al., 2005).

seis medidas propostas mais o objetivo do sistema em questão devem nortear a escolha do meio de prova a ser construído.

2.1.3 Sistemas Biométricos

Um Sistema Biométrico (SB) é essencialmente um sistema automático que reconhece a identidade de uma pessoa através de um dado biométrico. Em outras palavras, recebe um dado biométrico como entrada e tem como saída o reconhecimento positivo ou negativo de uma identidade. Um Sistema Biométrico genérico é dividido em 5 (cinco) subsistemas: Aquisição, Transmissão, Processamento, Base de Dados e Decisão (WAYMAN et al., 2005). A Figura 2.3 ilustra este SB genérico.

- Aquisição

Um SB começa com a aquisição do dado biométrico. A principal função do subsistema de Aquisição é garantir a acurácia do SB, independentemente das inúmeras variabilidades presentes no processo de aquisição. Para isso, este subsistema deve garantir a qualidade da captura do dado biométrico e não ser propenso a fraudes. Como apresentado na Figura 2.3, nesta etapa a biometria é apresentado para o dispositivo de aquisição, este

último a captura e repassa para o subsistema de Transmissão.

- Transmissão

O subsistema de Transmissão é responsável pela compressão, criptografia e protocolo de transmissão do dado adquirido até a unidade de processamento. Vale ressaltar que alguns SB armazenam completamente o dado adquirido, não passando por nenhum processamento.

- Processamento

O subsistema de Processamento é onde ocorre a segmentação, a extração de descritores e o controle de qualidade do dado biométrico. Nota-se que dependendo da qualidade da aquisição, o SB pode rejeitar a captura e proceder uma nova aquisição. Este subsistema gera uma representação para o dado biométrico e repassa-o para o subsistema Decisão ou paro o subsistema de Base de Dados, dependendo do modo de operação do SB.

- Base de Dados

Neste subsistema ficam armazenados os dados biométricos adquiridos ou as características deles extraídos. Vale ressaltar que a forma e o conteúdo armazenados afetam diretamente a velocidade de resposta do SB.

- Decisão

O subsistema de Decisão implementa política do SB, ou seja, determina os parâmetros que definem quando há o reconhecimento positivo ou negativo. Este limiar está intrinsecamente relacionado com o nível de exigência requerido pelo SB.

Observa-se que os 5 subsistemas supracitados estão fortemente relacionados com 5 etapas do PRIID. Desconsiderando os 5 subsistemas que compõem um SB e analisando o SB como uma unidade. Denota-se que o SB possui o objetivo de reconhecer a identidade, e portanto pode ser esquematizado da forma mostrada na Figura 2.4.

E também, o SB possui três modos de operações: registro, verificação e identificação. Os diagramas da figura 2.5 mostram as particularidades de cada um. O primeiro diagrama ilustra o registro da identidade formal e do dado biométrico, este é o momento em que acontece a correlação da biometria com a identidade. Só a partir daí, o sistema está apto a reconhecer. Os outros dois diagramas explicam a diferença entre verificação e identificação. Enquanto no primeiro, o usuário informa a sua identificação e apresenta a

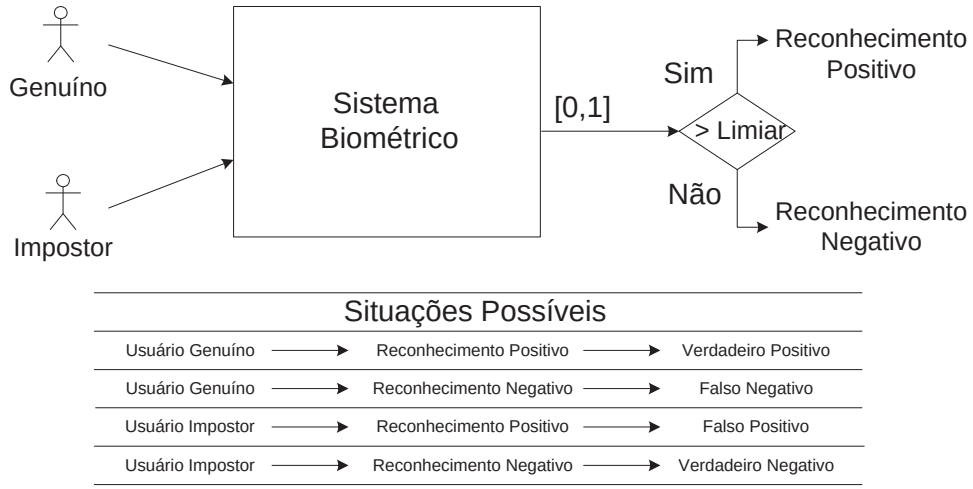


Figura 2.4: Situações possíveis de ocorrer em um Sistema Biométrico.

sua biometria, no segundo só há a apresentação do dado biométrico. Por conseqüência, a comparação feita na verificação é $1:1$ e na identificação e $1:N$.

2.1.3.1 Medidas de Desempenho

O SB tem como objetivo reconhecer a identidade de um indivíduo, para isso, a priori as saídas SB devem ser: Reconhecimento Positivo ou Reconhecimento Negativo. Apesar disso, os SB modernos não dão como saída um valor binário 0 para reconhecimento negativo ou 1 para reconhecimento positivo, e sim um valor real no intervalo $[0,1]$. Tendo como saída um valor neste intervalo, o SB também indica o grau de certeza do seu processo de reconhecimento. Quanto mais próximo de 1 mais certeza do reconhecimento positivo e vice-versa. Assim, cabe ao subsistema de Decisão sentenciar se reconhecimento foi positivo ou não através de um limiar. Quando a saída do SB for acima do limiar o reconhecimento seria positivo e abaixo o reconhecimento seria negativo. Esta forma de funcionamento melhora a robustez do SB, pois para aumentar ou diminuir o grau de exigência ou de precisão bastaria alterar o limiar.

As situações possíveis na interação de um usuário com um SB estão descritas na Figura 2.4. Nota-se que são quatro situações possíveis, duas desejadas e duas não desejadas. O falso positivo[4] e o falso negativo[5] são as situações a serem evitadas.

Deste modo, a acurária dos SB é determinada justamente pela ocorrência de

[4]Também chamado de Falsa Aceitação *(False Acceptance or False Match)*.

[5]Também chamado de Falsa Rejeição *(False Rejection or False Non-Match)*.

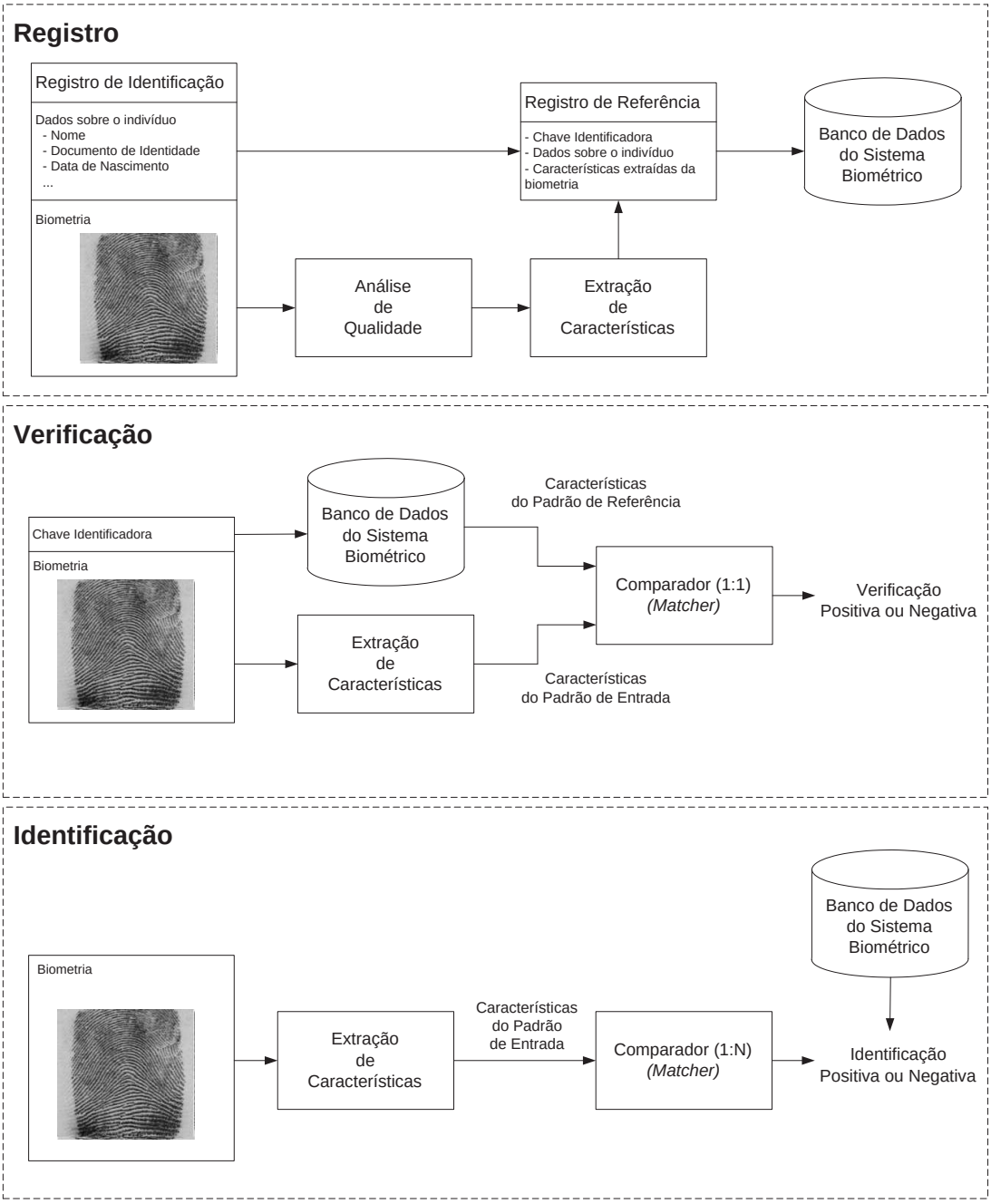


Figura 2.5: Modo de Operação dos Sistemas Biométricos - Registro, Verificação e Identificação

Falsa Aceitação e de Falsa Rejeição. Mas antes de discutir as medidas de desempenho, define-se o processo de reconhecimento de identidade por biometria a seguir.

Seja I a biometria apresentado pelo usuário e T a biometria anteriormente já adquirida na operação de Registro. Sendo H_0 o caso de um usuário impostor, se conclui que $I \neq T$. Sendo H_1 o caso de um usuário genuíno, de mesma forma se conclui que $I = T$. Assume-se $S(T,I)$ como função que calcula a similaridade entre a biometria adquirida e a biometria anteriormente registrada. Portanto, $S(T,I) \in [0,1]$, e por conseqüência, $S(T,I) = 0$ se T e I forem totalmente diferentes e $S(T,I) = 1$ se T e I forem idênticos. Então, o processo de reconhecimento pode ser definido por:

- Verificação

  Se $S(T,I) > Limiar$ Então H_1 Senão H_0

- Identificação

  $\forall\ T$: Se $S(T,I) > Limiar$ Então H_1 Senão H_0

É esperado que SB não falhe, logo seu desempenho de um SB é medido pela a ocorrência dos dois erros possíveis: Falsa Rejeição e Falsa Aceitação. A incidência de desses dois erros é medido pela Taxa de Falsa Rejeição (FRR) e pela Taxa de Falsa Aceitação (FAR), respectivamente. A primeira diz respeito à probabilidade de ocorrer Falsa Rejeição e é medida pela Equação 2.1, e a segunda é a probabilidade de ocorrer Falsa Aceitação e é determinada pela Equação 2.2.

$$FRR = \int_0^l p(s|H_1 = Verdadeiro)ds \tag{2.1}$$

$$FAR = \int_l^1 p(s|H_0 = Verdadeiro)ds \tag{2.2}$$

A Figura 2.8 mostra os valores de FRR e FAR graficamente. Nota-se que este gráfico é formado por duas curvas: a curva de Distribuição de Impostor e a curva de Distribuição de Genuíno (Legítimo). A curva de Distribuição de Impostor é determinada da seguinte forma: n usuários impostores se submetem m vezes ao SB, para cada submissão o SB irá produzir uma saída entre o intervalo $[0,1]$, a partir dessas saídas é construído um histograma onde o eixo das abscissa correspondem ao valor da saída e o eixo das coordenadas corresponde a quantidade de ocorrência de cada saída. A curva de Distribuição de Genuíno é determinada de modo análogo. Como se pode ver no gráfico da Figura 2.8, a curva de Distribuição de Impostor possui valores mais próximos de zero e a curva de

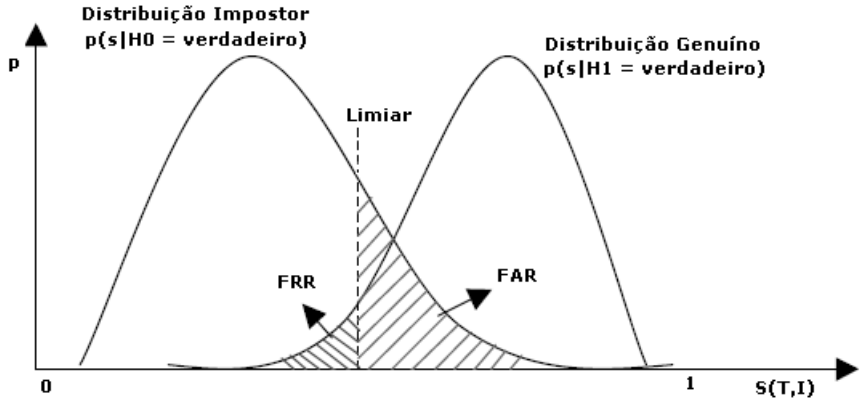


Figura 2.6: FAR e FRR para um dado limiar sobre as distribuições de Impostor e Genuíno. A área hachurada indicada por FAR determina a porcentagem de Falsa Aceitação e a indicada por FRR determina a porcentagem de Falsa Rejeição.

Distribuição de Genuíno possui valores mais próximos de um.

Outras métricas de avaliação de SB existente são: Taxa de Erro Igual (EER), Taxa de Zero Falsa Aceitação (ZeroFAR), Taxa de Zero Falsa Rejeição (ZeroFRR), Taxa de Falha no Registro, Taxa de Falha na Aquisição, Taxa de Falha no Reconhecimento. Essas métricas são apresentadas abaixo e são as mesmas utilizadas no critério de avaliação discutido no Capítulo 4.

- Taxa de Erro Igual (ERR)

Denota a taxa de erro onde o limiar (l) é tal que $FAR(l) = FRR(l)$ (Ver Figura 2.7).

- Zero FRR (ZeroFRR)

É a menor Taxa de Falsa Aceitação (FAR) tal que não ocorra Falsa Rejeição (Ver Figura 2.7).

- Zero FAR (ZeroFAR)

É a menor Taxa de Falsa Rejeição (FRR) tal que não ocorra Falsa Aceitação (Ver Figura 2.7).

- Taxa de Falha na Captura

É o percentual de falha ocorrida no processo de aquisição do dado biométrico. Ou seja, cada vez que o que o usuário submeter a sua biometria ao SB e este não capturá-la automaticamente com qualidade é um exemplo de Falha de Captura. Dispositivos de Capturas

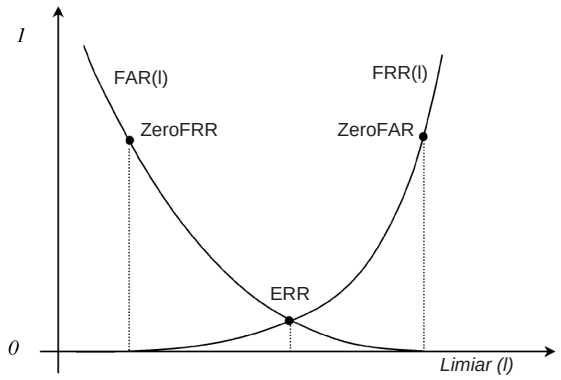


Figura 2.7: Exemplos de curvas FAR e FRR e os pontos ERR, ZeroFAR e ZeroFRR. (MALTONI et al., 2003)

robustos são aqueles com menor Taxa de Falha na Captura.

- Falha no Registro

É o percentual de falha ocorrida no processo de processamento do dado biométrico, isto é, qualquer erro cometido na etapa de segmentação ou na extração de descritores será computado como uma falha de registro. Vale ressaltar que um SB pode estabelecer níveis de qualidade dos dados biométricos capturados, para tanto um SB pode acusar falha no Registro quando a representação da biometria não atingiu a qualidade exigida.

- Falha no Reconhecimento

É o percentual de falha ocorrida no processo de reconhecimento *(matching)*. Normalmente, acontece quando o dado biométrico a ser reconhecido não atende o nivel de qualidade exigido.

2.1.3.2 Aplicações

Em princípio um sistema biométrico pode ser empregado aonde quer que seja necessário reconhecer a identidade de uma pessoa. Como já foi discutida, a segurança - seja ela patrimonial ou pessoal - justifica esta exigência de identificação a qualquer tempo e qualquer lugar. Daí surge a demanda por sistemas biométricos e eles cada vez mais estão presentes. É oportuno separar eles em duas áreas principais: Governamental & Forense e Comercial.

O âmbito onde o SB vai ser aplicado está fortemente relacionado com o nível de exigência requerido. Deste modo, é verdadeiro afirmar que os SB forenses tendem

Tabela 2.3: Exemplos de aplicações dos Sistemas Biométricos.

Governamental & Forense	**Comercial**
Identificação Civil	Acesso a Recursos Eletrônicos
Investigação Criminal	Controle de Ponto
Reconhecimento de Paternidade	Terminais Bancários
Controle de Fronteira	Atividade Comerciais

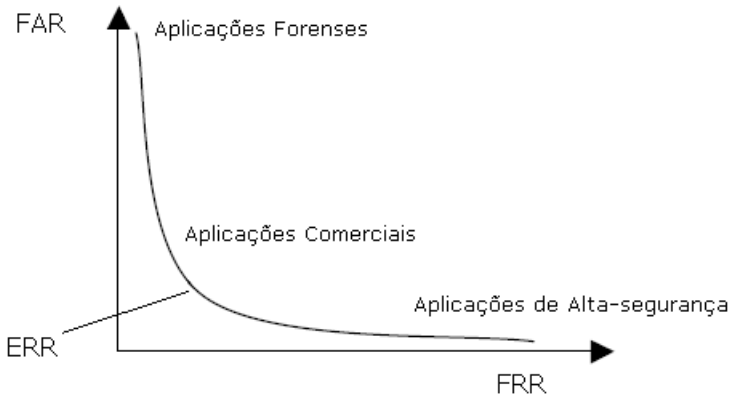


Figura 2.8: FAR e FRR esperados para cada tipo de aplicação.

admitir alta taxa de Falsa Aceitação para assim evitar o erro de Falsa Rejeição. Como normalmente, os SB forenses se concentram no reconhecimento de um indivíduo específico (autor de um crime), sempre haverá uma inspeção humana após a identificação. Portanto, é preferível ter uma dispendiosa inspeção a descartar uma possível identificação positiva que teria sido rejeitada caso houve um alta taxa de Falsa Rejeição. Para Aplicações de Alta-segurança acontece o contrário. Neste caso, busca-se baixa taxa de Falsa Rejeição, pois é melhor rejeitar o usuário legítimo a aceitar o impostor. A Figura 2.8 filustra a FAR e FRR esperados para cada tipo de aplicação.

2.2 Impressão Digital

A impressão digital é a biometria escolhida para o processo de reconhecimento de identidade a ser apresentado neste trabalho. As qualidades da ID como biometria fomentam a razão desta escolha. Como já anteriormente comentado a ID é de fácil coleta; é de grande alta aceitabilidade e pouco invasivo; possui métodos com bom desempenho de acerto; possui alta unicidade; é prático e seguro; grande porcentagem da população

está apta a oferecer esse dado biométrico; e por fim é uma forma de identificação com grande história de uso. A prova disso é que apesar de ser um método reconhecimento de identificação empregado a mais de um século, ainda é o mais prático, seguro e econômico que existe (FBI, 1984 apud COSTA, 2001). A seguir é descrito com maior detalhes as qualidades da ID.

1. **Boa Universalidade:** Uma grande porcentagem da população humana está apta em fornecer uma ID legível como um dado biométrico. Em outras palavras, a porcentagem dos indivíduos que possuem deficiência (ausência dos dedos) ou que possui ID ilegível é pequena. Sendo menor do que os que não possuem documento de identidade ou passaporte (CHIKKERUR, 2005).

2. **Alta unicidade:** A probabilidade de duas pessoas possuírem a mesma ID é muito próxima a zero. Até mesmo gêmeos idênticos possuem ID diferentes. Existem modelos matemáticos que provam esta alta unicidade (PANKANTI, 2002).

3. **Boa Imutabilidade:** As linhas da ID permanecem invariantes ao longo da vida, sendo apenas mudadas por fatores externos como queimaduras ou feridas.

4. **Facilidade de Coleta:** Cada vez é mais comum o uso de leitores *on-line* de impressão digital. Estes leitores de ID são capazes de capturar a imagem da ID em questão de segundos (CHIKKERUR, 2005). O treinamento requerido para manusear um leitor de ID é mínimo, independentemente se há vontade ou não do indivíduo a ser reconhecido.

5. **Alto Desempenho:** Sistemas biométricos baseados em ID alcançam desempenho superior aos demais.

6. **Boa Aceitabilidade:** Uma pequena porcentagem da população recusa em apresentar sua ID a fim de identificação. A ID é o tipo de biometria mais utilizada, mais da metade dos sistemas biométricos existentes no ano de 2002 utilizaram a ID como a biometria (MALTONI e al, 2003, p.12). Veja o gráfico da Figura 2.9.

2.2.1 História

Não é de agora que a ID começou a ser estudada. Há artefatos arqueólogos que ratificam o seu uso desde épocas antes de Cristo (MALTONI et al., 2003). Desde esta

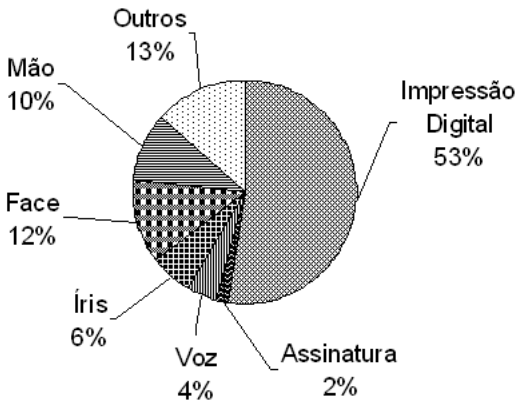


Figura 2.9: Participação dos Sistemas Biométricos que utilizam ID no mercado (2002).

época já havia evidências sobre a característica de unicidade da ID, contudo não havia base científica. Somente no século XVII, pelo trabalho do morfologista inglês Nehemiah Grew, houve um retorno ao estudo da ID. A partir deste momento inúmeros pesquisadores passaram a se interessar sobre impressões digitais como meio de identificação.

Em 1788, uma descrição detalhada da formação anatômica das ID for feita por Mayer, que identificou características peculiares das linhas da ID (MOENSSENS, 1971 apud MALTONI et al., 2003). Já em 1809, Thomas Bewick começou a utilizar sua própria ID como marca registrada (MOENSSENS, 1971 apud MALTONI et al., 2003). Purkinje, em 1823, propôs o primeiro esquema de classificação das ID (MOENSSENS, 1971 apud MALTONI et al., 2003). Em 1880, Henry Fauld, foi o primeiro a sugerir a unicidade da ID baseado em observações empíricas. No mesmo momento, Herschel afirmava que já teria empregado o reconhecimento de identidade por ID por 20 anos (LEE & GAESSLEN, 2001; MOENSSENS, 1971 apud MALTONI el al., 2003). Estes trabalhos foram o alicerce para as pesquisas sobre o reconhecimento de identidade por ID.

No final do século XIX, Sir Francis Galton conduziu um extensivo estudo sobre ID. E outro importante trabalho foi o de Edward Henry. Os trabalhos desses dois cientistas são um marco fundamental ao estudo da ID como biometria (MALTONI et al., 2003). Por fim, os inúmeros SB baseados em ID, bem como a literatura científica mostram o atual estado do estudo da ID.

2.2.2 Formação e Características

A pele é o órgão que cobre praticamente toda a parte externa do corpo humano, sendo que na palma das mãos, na sola dos pés e na parte interna dos dedos, ela adquire uma forma peculiar. Nestas regiões há um relevo sinuoso especial, formando uma espécie de onda senoidal, que possui a função de aumentar o atrito. A esta forma peculiar se dá o nome de papila. A Figura 2.10 retrata a estrutura da pele e mostra o relevo gerado pela papila. Nota-se que no topo deste relevo sinuoso estão as cristas e no fundo os vales. São exatamente as cristas ou linhas e os vales ou sulcos que caracterizam as impressões digitais, conforme mostrado na Figura 2.11. Por fim, vale destacar as regiões da ID, como está disposto na Figura 2.12. Basicamente, as informações mais importantes estão na região nuclear, esta é também a região que sofre menos distorção. Caso a ID seja adquirida pela sua rolagem a região marginal cresce, mas com distorção.

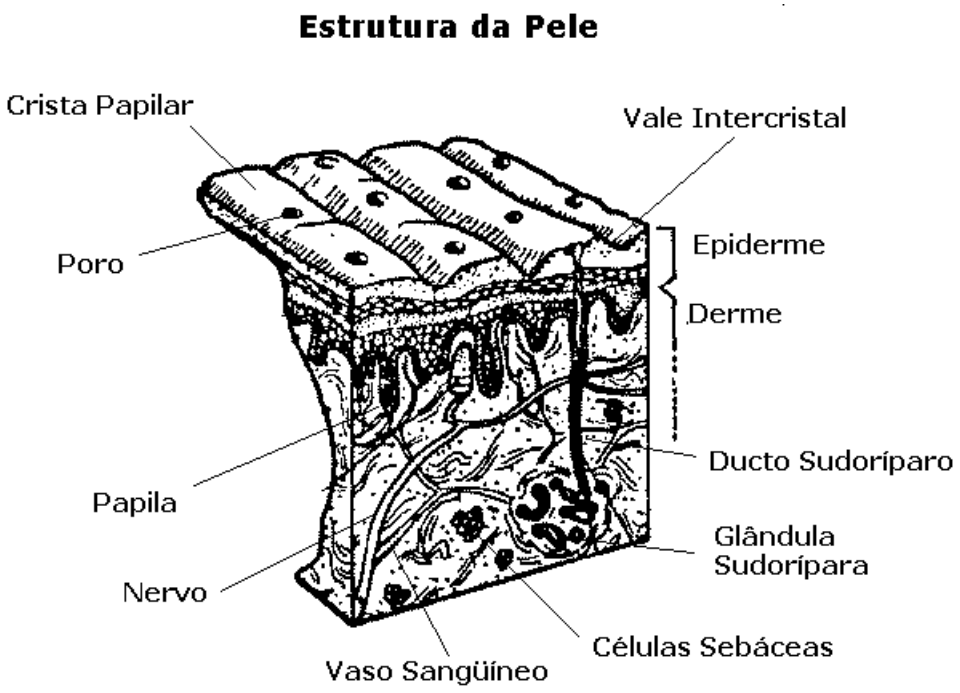


Figura 2.10: A estrutura da pele (JÚNIOR, 1991 apud KAZIENKO, 2003).

A formação da impressão digital se completa no sétimo mês de gestação, a partir deste momento o desenho formado pelas linhas e pelos vales permanece igual ao longo da vida, sendo modificado apenas por fatores externos como queimaduras e ferimentos (BABLER, 1991 apud MALTONI et al, 2003). Em princípio, as características de qualquer organismo biológico são frutos de interações entre os genes e o ambiente. Em

suma, um fenótipo[6], neste caso a ID, é determinado por uma interação de um específico genótipo[7] com uma específica condição do ambiente.

Sendo a ID um exemplo de fenótipo, ela é definida pelos genes e pelo ambiente. Enquanto os genes influenciam nas características da ID como a quantidade de cristas, a largura da crista, o espaço entre as linhas e a profundidade dos sulcos. É o ambiente, neste caso o fluxo de líquido amniótico, que define as características mais finas como a quantidade e a posição das descontinuidades das linhas. Como durante a gestação tanto a posição do feto no útero quanto o fluxo do líquido amniótico são aleatórios, isto faz que fator ambiente acrescente um componente aleatório na formação da ID (MALTONI et al., 2003). O que é provado pelo fato que as impressões digitais de gêmeos idênticos se diferenciam (JAIN et al., 2002). Esta corrobora a utilização da ID como biometria, pois mesmo outras biometrias como DNA, face e geometria da mão não são capazes de distinguir gêmeos uni vitelinos.

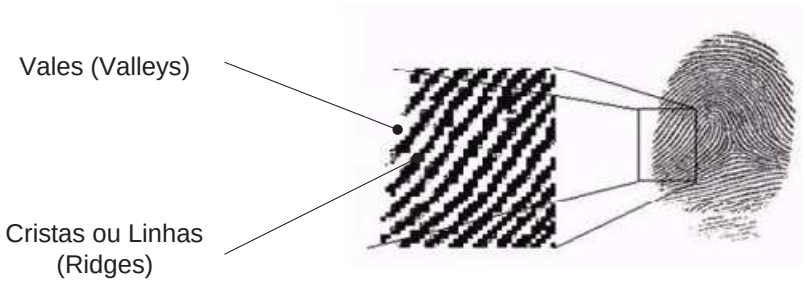


Figura 2.11: A ID, formada por cristas (linhas) e vales (sulcos).

Conforme mencionado na seção anterior, não é recente a história da ID. No percorrer do século XIX e XX, iniciou o estudo científico acerca dos desenhos formados pelas linhas da ID. Entre os colaboradores desses estudos destacam-se dois cientistas: Sir Francis Galton e Edward Henry. Pode-se dizer que ambos foram os precursores dos trabalhos científicos que envolvem a ID em um processo de identificação. O primeiro elaborou um trabalho meticuloso sobre as descontinuidades das linhas da ID. Estas descontinuidades deu-se o nome de minúcias[8] e elas são especialmente úteis para provar a unicidade de uma ID. O segundo versou a respeito dos desenhos especiais que as linhas da ID formam: as singularidades. As singularidades são os aspectos que definem as classes de ID. Até os

[6]Manifestação visível ou detectável de um genótipo.

[7]Composição genética de um indivíduo.

[8]Podendo também ser chamadas de *Galton deitails* em homenagem a Sir Francis Galton

dias de hoje se utilizam estas características observadas por estes dois cientistas (COSTA, 2001) (MALTONI et al., 2003) (MARQUES, 2004). Em parágrafos a frente elas serão aprofundadas.

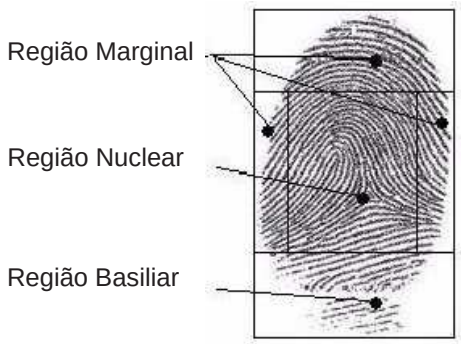


Figura 2.12: As regiões da ID.

A primeira aplicação da ID como prova de identificação ocorreu no âmbito forense. Na busca de identificar um criminoso através de ID latente a polícia instituiu peritos. Surge daí a papiloscopia. No início, a análise manual da ID era tarefa demorada e tediosa sendo necessário o uso de lentes de aumento e de um olho treinado (JAIN et al, 1997b; ELECCION, 1973 apud COSTA,2001). E somente com o emprego de recursos computacionais passou a ser viável o uso da ID em sistemas de autenticação. Portanto, a pesquisa sobre ID como meio de prova possui um base vinda da papiloscopia. Na sua dissertação de mestrado, Kazienko (2003) esclarece sobre papiloscopia e seu emprego, conforme a seguir.

> A papiloscopia, do latim papilla = papila e do grego skopein = examinar, é a ciência que estuda as impressões papilares e a identificação por meio das mesmas. Ela está dividida nas seguintes áreas: quiroscopia, podoscopia e dactiloscopia. A quiroscopia estuda a impressão da palma das mãos, ou seja, as impressões palmares. A palma da mão está dividida em quatro regiões anatômicas, a saber: digital, infradigital, tênar e hipotênar. A podoscopia estuda a impressão da planta dos pés, que esta é dividida em cinco regiões anatômicas, a saber: região do grande artelho, região do segundo ao quinto artelhos, região abaixo do grande artelho, região abaixo do segundo ao quinto artelhos e região do calcanhar. A dactiloscopia, do grego dáktylos = dedos e skopein = examinar, consiste em um método de identificação humana através da impressão digital. (KAZIENKO, 2003, p. 19)

As três principais áreas de atuação da dactiloscopia são (KAZIENKO, 2003):

- **Dactiloscopia Civil** - Trata da identificação para fins civis, como a carteira de iden-

tidade;

- **Dactiloscopia Criminal** - Nesta área encontram-se as três possibilidades. A identificação do indiciado em inquérito policial não identificado anteriormente ou quanto houver dúvida ou suspeita sobre sua identidade; a de documentos de idoneidade como o atestado de antecedentes criminais e folha de antecedentes e a de fragmentos de impressões digitais encontradas em locais de crime;

- **Dactiloscopia Clínica** - Cuida do estudo sobre as perturbações observadas nos desenhos digitais em conseqüência de algumas doenças ou do exercício de certas profissões.

Por fim, na figura 2.13 é apresentado a impressão digital e suas características. Nesta ilustração são mostrados exemplos de singularidades, de minúcias e os poros. Este último é dificilmente utilizado por exigir imagens de ID de alta resolução. Nas seções seqüentes são expostos os principais tipos de características a serem extraídas de uma ID, destacam-se os dois tipos mais usados: as singularidades e as minúcias.

Figura 2.13: As singularidades e as minúcias de uma ID.

2.2.2.1 Singularidades

Conforme já mencionado, a ID é formada por linhas e vales, entretanto quando se analisa a ID como um conjunto de linhas e de vales percebe-se que este conjunto as-

sume uma forma peculiar. Este desenho formado pelas linhas pode ser distinguido por uma curva acentuada, por espécie de espiral ou por uma divergência. Estes desenhos particulares estão presentes em quase toda totalidade das ID, elas não servem como identificadores, mas sim como classificadores. Os pontos especiais dessas formas peculiares são chamados de singularidades ou pontos singulares.

Na Figura 2.13 existe dois tipos de singularidades: núcleo[9] e delta. O núcleo se divide em dois subtipos: ápice *(loop)* e *whorl* (MALTONI et al., 2003). O ápice é aquela curva mais acentuada, o *whorl* é a espiral e o delta é onde as linhas formam uma espécie de ângulo ou triângulo. No entanto estas definições não são fortes o suficiente para determinar uma singularidade. As Figuras 2.14 e 2.15 mostram exemplos de configurações das singularidades delta e núcleo, respectivamente.

Figura 2.14: Exemplos de configurações da singularidade Delta (HONG, 1998).

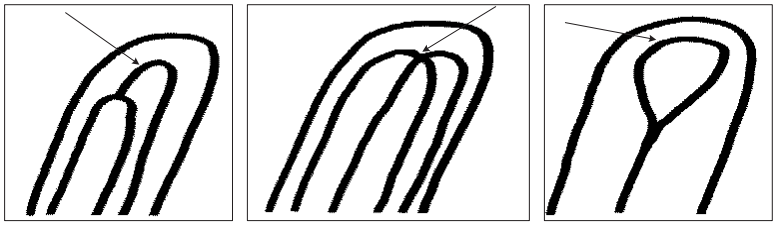


Figura 2.15: Exemplos de configurações da singularidade Núcleo (HONG, 1998).

O propósito de detecção das singularidades é tanto para classificação da ID quanto para auxiliar o reconhecimento. Com a classificação se reduz o espaço de busca de ID a serem confrontadas nos casos de identificação, ou seja, a comparação só dar-se-á entre ID pertencentes a mesma classe. Já no processo de verificação, os pontos singulares podem servir como referências as demais características ou pode ser o ponto de equivalência entre duas ID. O Capítulo 4 possui exemplos de técnicas de verificação que utilizam as singularidades.

[9]Do inglês *core.*

Em relação aos tipos de classes de ID existentes predomina as classes definidas pelo Sistema Henry. Esse sistema categoriza as ID em 5 classes, a saber: Arco Plano *(Plain Arch)*; Arco Angular *(Tented Arch)*; Presilha Interna ou Presilha Direita *(Left Loop)*; Presilha Externa ou Presilha Esquerda *(Right Loop)*; e Verticilo *(Whorl)* (COSTA, 2001), (LIMA, 2002) e (MARQUES, 2004). Outros autores simplificam e tratam as classes Arco Plano e Arco Angular como sendo uma classe só, a classe Arco. Poucas são as ID que não se enquadram a essas classe, no entanto, se ocorrer a ID é categorizada na classe Acidental. Descreve-se a abaixo essas 5 classes (COSTA, 2001) (MALTONI et al., 2003).

- **Arco Angular** - nesta classe as linhas atravessam a ID de um lado ao outro com acentuada elevação no centro, há um ápice e um delta;

- **Arco Plano** - as linhas atravessam a ID de um lado ao outro com uma pequena elevação no centro, não possui pontos singulares;

- **Presilha Externa ou Esquerda** - as linhas vêm de um lado e podem voltar para o mesmo lado, os pontos singulares delta e ápice estão presentes, sendo que o delta aparece à esquerda do ápice *(loop)*;

- **Presilha Interna ou Direita** - parecida com a classe anterior, a única diferença é que o delta está à direita do ápice *(loop)*;

- **Verticilo** - nesta classe há pelo menos uma linha que faz um giro de 360 graus, podendo assumir uma forma de espiral ou um duplo ápice, pode conter dois deltas e dois ápices.

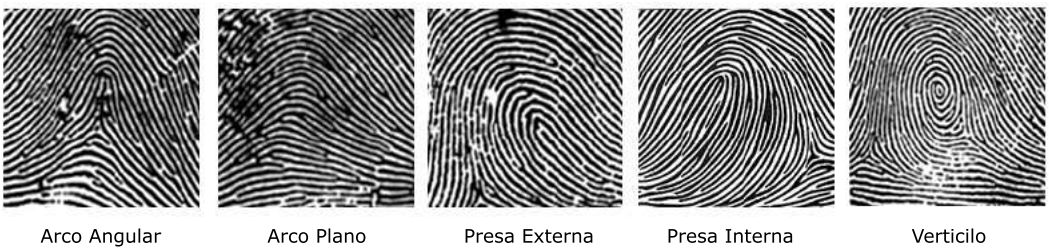


Figura 2.16: Tipos de classes do Sistema Henry (CHIKKERUR, 2005).

A Figura 2.16 ilustram as classes do Sistema Henry e a tabela 2.4 apresenta a percentagem de ocorrência de cada uma dessas classe na população em geral (WILSON, CANDELA & WATSON, 1994 apud MALTONI et al, 2003).

Tabela 2.4: Distribuição das classes de ID (WILSON, CANDELA & WATSON, 1994 apud MALTONI et al, 2003).

Classe da ID	**Frequência Média**
Arco Angular*(Tented Arch)*	$3,7\%$
Arco Plano*(Arch)*	$2,9\%$
Presilha Direita *(Left Loop)*	$33,8\%$
Presilha Esquerda *(Right Loop)*	$31,7\%$
Verticilo *(Whorl)*	$29,7\%$

2.2.2.2 Minúcias

As minúcias são características de maior relevância a serem extraídas da ID. Elas foram inicialmente estudas por Sir Francis Galton no ano de 1982, e até hoje elas continuam sendo os principais atributos utilizados nos métodos reconhecimento de identidade por ID (MALTONI et al., 2003). Uma minúcia é uma descontinuidade presente em uma linha da ID, isto é, é uma interrupção existente no caminho de uma linha. Em seu livro, Maltoni et al (2003) descrimina os tipos de minúcias existentes conforme ilustrado na Figura 2.17.

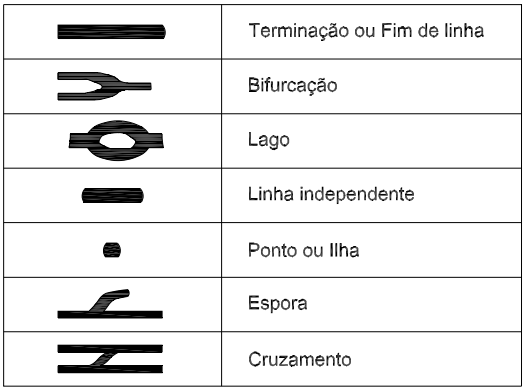


Figura 2.17: Os tipos de minúcias (MALTONI et al., 2003).

Já Costa (2001) categoriza as minúcias de outras duas formas: aspectos sim-

Tabela 2.5: Distribuição das minúcias (COSTA, 2001).

Tipos de Minúcias	**Freqüência Média**	
	% do total de Minúcias	**Minúcias Por impressão**
Terminação *(ridge ending)*	60,6	258
Bifurcação *(birfucation)*	17,9	76
Linha independente *(independent ridge)*	6,1	26
Espora *(spur)*	4,7	20
Ponto *(dot)*	4,3	18
Cruzamento *(crossover)*	3,2	14
Ponte *(bridge)*	2,5	10
Ilha *(island)*	0,7	3

ples e aspectos compostos. Os aspectos básicos seriam as cristas finais ou terminação[10] (fim-de-linha) e as crista bifurcadas ou bifurcação[11]. Os aspectos compostos seriam determinados pelos aspectos básicos, isto é, seriam casos especiais dos aspectos básicos (HRECHAK et al, 1990 apud COSTA, 2001). Por exemplo, a minúcia lago seria um exemplo de duas bifurcações próximas como se pode concluir pela Figura 2.17. A tabela 2.5 mostra a ocorrência média de cada tipo de minúcias em uma ID. Os dados desta tabela servem de parâmetros de avaliação para um processo de extração de minúcias. Apesar de se encontrar vários tipos de minúcias em ID, apenas a terminação e bifurcação são os tipos empregados em um PRIID. Esta simplificação ocorre em razão a possível confusão entre um ruído da imagem e as minúcias dos outros tipos, o que causa pouco impacto, pois mais de $3/4$ das minúcias são dos tipos bifurcação e terminação (ver Tabela 2.5).

É destacado na Figura 2.13 algumas das minúcias desta imagem. Nota-se que em um exame visual se consegue localizar as minúcias, não obstante, a dificuldade desse exame é inversamente proporcional a qualidade da imagem. Em outras palavras, se qualidade da imagem for ruim possivelmente o processo de extração de minúcia irá selecionar minúcias espúrias. Outras considerações acerca da detecção de minúcias serão comentadas no próximo capítulo.

Como já dito, o conjunto de minúcias de uma ID é a principal representação de ID empregada no PRIID, sendo a bifurcação e a terminação os únicos tipos de minúcias considerados. E cada minúcia é denotada por um vetor composto por 4 características

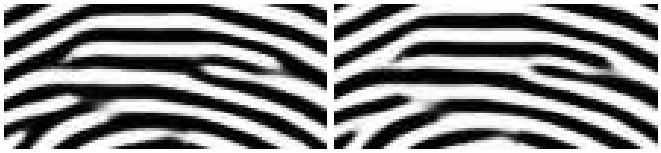
[10]Do inglês *ridge ending*.

[11]Do inglês *bifurcation*.

(ver Figura 2.19): o tipo da minúcia, a sua posição em relação ao eixo x, a sua posição em relação ao eixo y e o seu ângulo em relação a horizontal. A equação 2.3 mostra a representação da ID como um conjunto de minúcias.

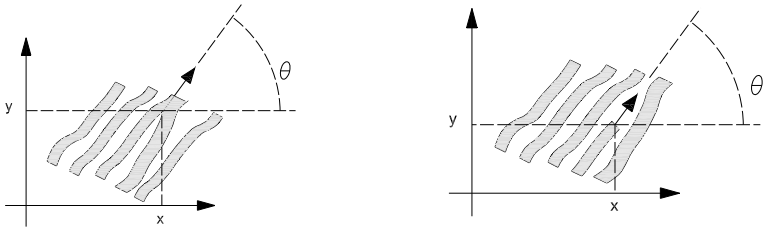
$$ID = \{m_1, m_2, \ldots, m_n\}, \quad m_i = \{T_i, x_i, y_i, \theta_i\}, \quad i = 1 \ldots n \tag{2.3}$$

Apesar do tipo de minúcia ser um atributo contido na notação acima, nem todos os métodos de reconhecimento o consideram. Isto é explicado pelo fato de uma bifurcação se transformar em uma terminação ao se inverter a imagem da ID, a Figura 2.18 mostra esta propriedade. Sendo assim, houve uma preocupação quanto a forma de extração dos atributos da uma minúcia, isto é, as minúcias extraídas de uma imagem de ID qualquer e a imagem negativa correspondente terão atributos equivalentes exceto relação ao tipo (Figura 2.19).



(a) Imagem Normal (b) Imagem Negativa

Figura 2.18: Na imagem negativa o que era terminação vira bifurcação e vice-versa.



(a) Bifurcação - (x, y, θ) (b) Terminação - (x, y, θ)

Figura 2.19: As duas minúcias principais e suas representações

2.2.2.3 Outras Características

Além dos pontos singulares e das minúcias, outras características podem ser extraídas das ID afim de auxiliar o PRIID. Como, por exemplo, as posições, as formas e a quantidade de poros em uma ID (Figura 2.13). Em seu trabalho Stosz & Alyea (1994, apud MALTONI et al, 2003) propõem um método de autenticação baseado nos poros e nas

estruturas das linhas, contudo apesar dos poros serem informações capazes de distinguir a individualidade, pesa desfavoravelmente o fato de que só em imagens de alta qualidade é possível a visualização dos poros.

Outra característica possível de ser extraída é a quantidade de linhas entre duas posições definidas. Normalmente essa duas posições são duas minúcias, um ponto singular e uma minúcia ou vice-versa. A Figura 2.20 ilustra esta característica. Além de este dado ser de fácil determinação, conta ao seu favor a sua independência em relação à posição e a rotação da ID, isto é, a quantidade de linhas entre minúcias permanece a mesma não importando a posição da apresentação da digital sobre o dispositivo de coleta, o que não ocorrem com as minúcias.

Figura 2.20: A quantidade de linhas entre duas minúcias

Apesar das características discorridas até aqui compreenderem quase todo universo das características empregadas em um PRRID, há trabalhos que aproveitam outras informações disponíveis em uma ID, como a forma da linha, a textura, a freqüência e a orientação das linhas em uma região definida e etc. Para finalizar, é válido ressaltar que o método de reconhecimento está intrinsecamente relacionado com qual informação foi extraída da ID.

2.2.3 Individualidade

Popularmente, a impressão digital é tida como sinônimo de algo que representa a unicidade de uma pessoa. Contudo, este pensamento veio de observações práticas sem ter nenhuma certeza matemática. Mesmo assim, a sociedade - principalmente as instituições jurídicas - tomou como verdade a premissa que não há duas ID iguais, o que fez considerar uma ID latente como prova jurídica lícita a ser aplicada na comprovação de identidade de um indivíduo. Não se indagava acerca desta veracidade aparente, pois

ela sempre foi legitimada pela comunidade científica, conforme as afirmações a seguir (MALTONI et al., 2003).

> Only once during the existence of our solar system will two human beings be born with similar finger markings - Harper's headline, 1910.
>
> Two like fingerprint would be found only once every 10^{48} years - Scientific American, 1911.

No entanto, houve um processo na corte americana que questionou a veracidade de uma ID ser algo realmente único. A partir deste momento, surgiu a necessidade de obter uma certeza matemática sobre essa questão. Ao que parece, Galton foi o primeiro cientista que, em seu trabalho propôs uma forma de se estimar esta probabilidade, baseando-se nos desenhos das linhas da impressão digital (MARQUES, 2004).

Tabela 2.6: Probabilidades de haver dois indivíduos distintos com a mesma impressão digital, exigindo que representação da ID contenha um Conjunto de 12 minúcias, 8 regiões definidas por Galton e 24 regiões definidas por Osterburg et al. (PANKANTI, 2002)

Autor	**Probabilidade**
Galton (1892)	1.45×10^{-11}
Henry (1900)	1.32×10^{-23}
Balthazard (1911)	2.12×10^{-22}
Bose (1917)	2.12×10^{-22}
Wentworth & Wilder (1918)	6.87×10^{-62}
Pearson (1930)	1.09×10^{-41}
Roxburgh (1933)	3.75×10^{-47}
Cummins & Midlo (1943)	2.22×10^{-63}
Trauring (1963)	2.47×10^{-26}
Gupta (1968)	1.00×10^{-38}
Osterburg et al (1977)	1.33×10^{-27}
Stoney (1985)	1.20×10^{-80}

Em princípio, em um nível microscópio não há dois objetos idênticos. Numa visão microscópia sobre dois objetos ditos como idênticos, perceber-se-ia que a superfície de cada objeto teria uma forma distinta. Desta forma, o importante não é verificar a unicidade de uma ID, e sim aferir se os métodos de reconhecimento de ID são precisos o suficiente para garantir esta unicidade. Isto é, o método de reconhecimento deve coletar uma quantidade suficiente de características da ID de forma a garantir que ID identifica uma só pessoa.

Em seu artigo, Pankanti et al. (2002) apresenta estudos que discorrem sobre

o que e o quanto é preciso extrair de uma ID a fim de assegurar um reconhecimento incontestável. Também, demonstra que se um par de ID contiver 12 minúcias coincidentes - em posição e ângulo - a probabilidade dessas duas ID serem de indivíduos distintos é ínfima. Neste mesmo artigo é apresentado vários trabalhos, com diferentes enfoques, que tratam do cálculo desta probabilidade e os resultados desses trabalhos estão expostos na Tabela 2.6.

Por fim, Pankanti et al. (2002) chegam nas seguintes conclusões: ao contrário da crença popular, o reconhecimento de identidade não é infalível; existe uma quantidade suficiente de informações na ID que a tornam única, no entanto devido a ruídos e a resolução dos dispositivos de aquisição essa informações não são totalmente capturadas; o desempenho do processo de reconhecimento está muito longe do limite teórico e por só utilizar minúcias os PRIID não usam toda informação que distinguem as ID; é desejável a estes sistemas empregarem outras informações.

2.3 Considerações Finais

Foi o objetivo deste capítulo expor o estado da arte sobre o tema biometria, mais especificamente a impressão digital, bem como apresentar os Sistemas Biométricos. Ambos os assuntos são de extremo interesse à comunidade acadêmica, às instituições governamentais e às empresas comerciais. O que é explicado pela alta aplicabilidade dos Sistemas Biométricos. Tanto é assim, que todas as entidades interessadas estabeleceram organismos que regulamentam e avaliam os Sistemas Biométricos.

Um exemplo desta integração destas entidades foi a criação de uma competição de verificação de ID (FVC)[12]. Esta competição é aberta a instituições educacionais e empresas comerciais. Nela cada um dos competidores submete seus algoritmos a fim de avaliar a acurácia dos mesmos. Outro exemplo da integração é o serviço de certificação de *AFIS* prestado pela Polícia Federal Americana (FBI). Uma certificação do FBI ratifica uma qualidade do aplicativo em questão. A Tabela 2.7 apresenta os principais grupos de pesquisa, instituições governamentais e organizações internacionais atuantes na área de biometria.

[12] *Fingerprint Verification Competition*

Tabela 2.7: Exemplos de grupos de pesquisa, intituições governamentais e organizações internacionais.

Grupos de Pesquisa	**URL**
ATVS Universidade Autonôma de Madri - Espanha	http://atvs.ii.uam.es/
BIOLAB - Biometric System Laboratory Universidade de Bologna - Itália	http://biolab.csr.unibo.it/
National Biometric Test Center Universidade de San José - EUA	http://www.engr.sjsu.edu/biometrics/
PRIP - Biometrics Research Universidade do Estado de Michigan - EUA	http://biometrics.cse.msu.edu/
Instituições Governamentais	**URL**
FBI Federal Bureau of Investigation	http://www.fbi.gov/hq/cjisd/iafis/cert.htm
National Institute of Standards and Technology	http://www.itl.nist.gov/
Organizações Internacionais	**URL**
Biometrics Catalog	http://www.biometricscatalog.org/
Biometric Consortium	http://www.biometrics.org/
International Biometric Group	http://www.ibgweb.com/

3 ESTUDO DE TÉCNICAS UTILIZADAS NO PROCESSO DE RECONHECIMENTO DE IDENTIDADE POR IMPRESSÕES DIGITAIS

Como o próprio título deste capítulo expõe, a seguir são apresentadas as principais técnicas utilizadas no PRIID. O estudo se concentra na etapa de extração de características da ID e também na etapa de verificação onde acontece a comparação de dois conjuntos de características extraídas da ID com o objetivo de se verificar se estes dois conjuntos pertencem ao mesmo indivíduo. Por fim, é exposto o protótipo concebido e implementado de um sistema de verificação de identidade por impressões digitais.

Antes de abordar estes temas será feita uma breve exposição sobre alguns tópicos da área de processamento de imagens digitais que são utilizados tanto nos algoritmos de extração de características como no processo de verificação.

3.1 Tópicos em Processamento de Imagens

Conceitualmente, processamento de imagens digitais reúne inúmeras técnicas e algoritmos computacionais construídos para manipular imagens digitalizadas tanto em 2 (duas) como em 3 (três) dimensões (BARBOZA, 2005). Dentre os objetivos de manipular imagens se sobressaem o de melhoria da qualidade da informação visual da imagem de forma a facilitar a interpretação humana e o que visa processar a imagem com a finalidade de possibilitar a percepção automática do seu conteúdo por máquinas (GONZALEZ & WOODS, 2000).

É crescente o uso de técnicas de processamento de imagens, fato este justificado pelas inúmeras áreas de aplicação, como por exemplo, na Arqueologia (recuperação visual de artefatos danificados), na Biologia (análise de organismos microscópicos), na

Criminalística (identificação de vítimas ou criminosos), na Defesa (radares e sonares utilizados na identificação de alvos ou inimigos), na Geologia (estudo de relevo e formações rochosas em larga escala), na Medicina (radiologia, ressonância magnética, tomografia computadorizada e ultra-sonografia) entre outras (JAIN, 1989; GONZALEZ & WOODS, 2000 apud BARBOZA, 2005).

3.1.1 Representação da Imagem

Para o computador interpretar uma imagem é necessário um processo de digitalização e decodificação. Uma imagem digital monocromática é formada por um conjunto de *pixels* (Equação 3.1), onde (x,y) é a coordenada de um *pixel* qualquer da imagem e I é a sua respectiva intensidade de luz (luminância). Esta luminância refere-se a quantidade de luz incidente no ambiente e a reflectância dos objetos presentes neste ambiente, podendo ser determinada pela equação 3.2, sendo i a incidência de luz e r a reflectância do objeto.

$$I = \{f(x,y)\} \tag{3.1}$$

$$f(x,y) = i(x,y) \,.\, r(x,y) \tag{3.2}$$

Em termos físicos a luminâcia é uma grandeza contínua e o números de *pixels* de uma imagem não possui limites, desta forma, para ser possível sua representação computacional, é preciso estabelecer limites para o número de *pixels* (resolução da imagem) e discretizar a luminânica. Amostragem e quantificação são, respectivamente, os nomes desses processos. A amostragem define a resolução da imagem, já a quantificação corresponde a quantidade de tons de cinza usados para representar a luminância (geralmente 8 *bits* que possibilita 256 tons de cinza) (BARBOZA, 2005). Ambas são definidas pelas equações 3.3 e 3.4 , respectivamente:

$$\begin{cases} 0 \leq x < W, \text{onde W representa a largura da imagem} \\ 0 \leq y < H, \text{onde H representa a altura da imagem} \end{cases} \tag{3.3}$$

$$f(x,y) \in \{0,1,2,3,4,\ldots,2^n\} \; \forall \; x,y \mid 0 \leq x < W \;\; e \;\; y < H \tag{3.4}$$

Em termos de implementação, uma imagem monocromática pode ser definida como um matriz bidimensional $(W \times H)$, onde W é a largura e H é a altura. A Figura

3.1 exemplifica esta representação. A imagem nesta figura seria definida por uma matriz (18×12), cada quadrado representa um *pixel* e por ser uma imagem em tons de cinza os valores possíveis de cada *pixel* são de 0 a 255 ou 0 a 1. Observa-se que por convenção a origem da coordenadas é o canto superior esquerdo da imagem.

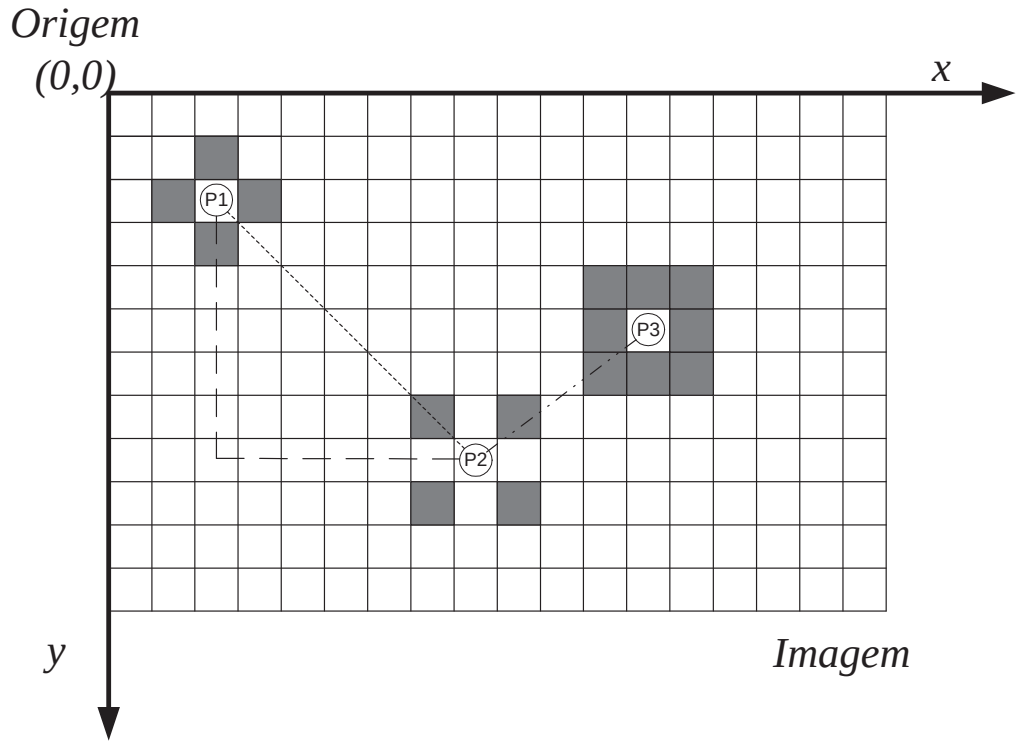


Figura 3.1: Representação matricial de uma imagem monocromática bidimensional.

3.1.2 Relação entre Pixels

Definida a representação matricial da imagem, fica claro que processar uma imagem digital monocromática se resume a manipular uma matriz de *pixels*, cada um com valores entre 0 e 255. As principais relações entre os *pixels* de uma imagem são:

3.1.2.1 Vizinhança

A relação de vizinhança entre *pixels* é determinada pelo posicionamento dos *pixels* de uma imagem. São 3 os principais tipos de vizinhança entre *pixels* de uma mesma imagem. São eles: vizinhança-de-4, vizinhança diagonal e vizinhança-de-8 (GONZALEZ & WOODS, 2000).

- **Vizinhança-de-4**: os vizinhos-de-4 de um *pixel* p qualquer correspondem aos *pixels* vertical e horizontalmente adjacentes a p. Considerando então $p = (x;y)$, o conjunto dos vizinhos-de-4 de P, denotado por $N_4(p)$, seria formado por $(x-1;y)$; $(x+1;y)$; $(x;y-1)$ *e* $(x;y+1)$. Na Figura 3.1 os vizinhos-de-4 do *pixel* $P1$ são exatamente os quatro *pixels* cinzas em volta dele.

- **Vizinhança-diagonal**: analogamente, os vizinhos diagonais de p são aqueles diagonalmente adjacentes ao mesmo. Sendo assim, $N_D(p)$ consistiria de $(x-1;y-1)$; $(x-1;y+1)$; $(x+1;y-1)$ *e* $(x+1;y+1)$. Na Figura 3.1 os vizinhos diagonais do *pixel* $P2$ são os quatro *pixels* cinzas em volta dele.

- **Vizinhança-de-8**: o conjunto de vizinhos-de-8 de p corresponde a união entre os conjuntos $N_4(p)$ e $N_D(p)$. Sendo assim, $N_8(p) = N_4(p) \cup N_D(p)$. Na Figura 3.1 os oito *pixels* cinzas em volta do *pixel* $P3$ são seus vizinhos-de-8.

3.1.2.2 Conectividade

Outra relação importante é a conectividade entre *pixels*. Esta relação é extremamente útil no processo de detecção de bordas de objetos e no processo de determinação de componentes em uma imagem. Dois *pixels* quaisquer estão conectados quando há um caminho de *pixels* entre esses dois que atenda uma determinada condição. Cada passo do percurso deste caminho é feito a algum *pixel* adjacente, respeitando a relação de vizinhança e o nível de similaridade da conectividade pretendida. Dois *pixels* conectados devem atender uma similaridade S (p. ex., níveis de cinza) e uma vizinhança V (p. ex, vizinhança-de-4). Abaixo é descrito quatro tipos de conectividade (BARBOZA, 2005):

- **Conectividade-de-4**: dois *pixels* p e q estão conectados-de-4 se atendem uma similiaridade S e $q \in N_4(p)$;

- **Conectividade-Diagonal**: dois *pixels* p e q estão conectados de diagonal se atendem uma similaridade S e $q \in N_D(p)$;

- **Conectividade-de-8**: dois it pixels p e q estão conectados-de-8 se atendem uma similaridade S e $q \in N_8(p)$;

- **Conectividade-de-m (conectividade mista)**: dois *pixels* p e q estão conectados-de-m se atendem uma similaridade S e $q \in N_4(p)$ ou $q \in N_D(p)$ e o conjunto $N_4(p) \cap N_4(q)$.;

Junto com a relação de conectividade entre *pixels* aparecem os conceitos de comprimento do caminho e de componente conexo. Gonzalez & Woods (GONZALEZ & WOODS, 2000) definem o conceito de caminho da seguinte forma.

> Um caminho de um *pixel* p com coordenadas (x,y) a um *pixel* com coordenadas (s,t) é uma seqüência de *pixels* distintos com coordenadas $(x_0,y_0),(x_1,y_1),\ldots,(x_n,y_n)$ em que $(x_0,y_0)=(x,y)$ e $(x_n,y_n)=(s,t)$ é adjacente a $(x_{i-1},y_{i-1},\ 1\leq i\leq n$, e n é o *comprimento* do caminho. Podemos definir caminhos-de-4, -8 ou -m, dependendo do tipo de adjacência especificado. (GONZALEZ & WOODS, 2000, p. 29)

E o conceito de componente conexo da forma abaixo.

> Se p e q forem *pixels* de um subconjunto S de uma imagem, então p está *conectado* a q em S se existir um caminho de p a q consistindo inteiramente de *pixels* S. Para qualquer *pixel* p em S, o conjunto de *pixels* em S que estão conectados a p é denominado um *componente conexo* de S.

3.1.2.3 Distância

A distância entre *pixels* é outra relação importante. Dado três *pixels* p, q e r quaisquer, com coordenadas (x,y), (s,t) e (u,v) respectivamente, D é uma medida de distância se:

1. $D(p,q)\geq 0$;
2. $D(p,q)=0$ *se e somente se* $p=q$;
3. $D(p,q)=D(q,p)$;
4. $D(p,r)\leq D(p,q)+D(q,r)$.

Os tipos de medidas de distância mais comuns são: a distância Euclidiana; distância D_4 (Manhattan) e distância D_8 (Xadrez). As suas definições são dadas abaixo:

- **Distância Euclidiana**: $D_e(p,q)=\sqrt{(x-s)^2+(x-t)^2}$
- **Distância** D_4: $D_4(p,q)=|x-s|+|y-t|$
- **Distância** D_8: $D_8(p,q)=max(|x-s|,|y-t|)$

Na Figura 3.1, a distância D_4 está indicada pelo o segmento tracejado (traço-longo) que liga o *pixel* $P1$ ao *pixel* $P2$, a distância D_8 está indicada pelo segmento tracejado (traço-curto) que liga o *pixel* $P1$ ao *pixel* $P2$ e a distância D_e está indicada pelo segmento (traço-ponto-traço) que liga o *pixel* $P2$ ao *pixel* $P3$.

3.1.2.4 Operações, Transformações e Filtros

Para finalizar esta seção, é exposto algumas das principais operações e transformações empregadas no processamento de imagem. As obras de Gonzalez & Woods (2000) e de Jain (1988) discorrem este assunto com maior profundidade.

Dentre as operações aplicadas sobre uma imagem destacam-se as operações lógico-aritméticas. As operações aritméticas são a soma, a subtração, a multiplicação e a divisão. As operações lógicas são geralmente aplicadas sobre uma imagem binária, elas são: E (AND), OU (OR), OU-Exclusivo (XOR) e Negação (NOT). Estas operações são aplicadas *pixel* a *pixel* ou entre *pixels* de imagens distintas. A Figura 3.2 ilustra um exemplo da operação de multiplicação e a Figura 3.3 um exemplo de Negação (BARBOZA, 2005).

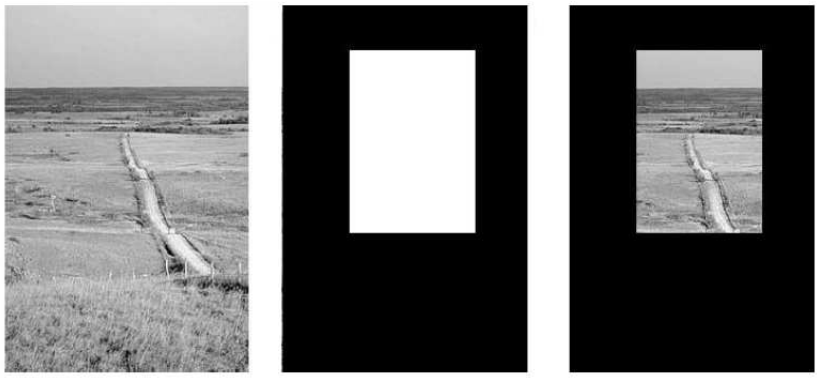
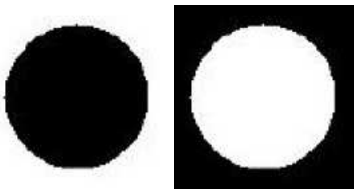


Figura 3.2: Exemplo da aplicação da operação de multiplicação para destacar uma determinada região em uma imagem (BARBOZA, 2005).



(a) (b)

Figura 3.3: Exemplo da aplicação da operação de negação (NOT) (BARBOZA, 2005)

A respeito das transformações sobre as imagens, existem duas categorias principais: transformações geométricas e transformações radiométricas. A primeira atua sobre a distribuição dos *pixels*, e a segunda categoria atua na luminância dos *pixels* (BARBOZA, 2005). O escalamento (redução ou ampliação), a translação e a rotação são exem-

plos de transformações geométricas. A limiarização, a expansão e a equalização de histograma são exemplos de transformações radiométricas (BARBOZA, 2005).

O histograma de uma imagem corresponde a uma representação dos níveis de cinza contidos em uma imagem, podendo ser visto como uma função de densidade dos mesmos na imagem (WINKLER & THOMÉ, 2003 apud BARBOZA, 2004). Para uma imagem codificada em n bits, ter-se-ia $2n$ níveis de cinza possíveis, variando de 0 (zero) a $2^n - 1$. A construção do histograma é constituída do estabelecimento de uma relação entre cada nível de cinza possível e o número de vezes que ele aparece na imagem. A equalização do histograma corresponde a tentativa em alterar a distribuição do histograma de forma que o mesmo se aproxime a uma distribuição uniforme. A Figura 3.4 ilustra uma imagem e seu respectivo histograma, já a Figura 3.5 apresenta a equalização de histograma.

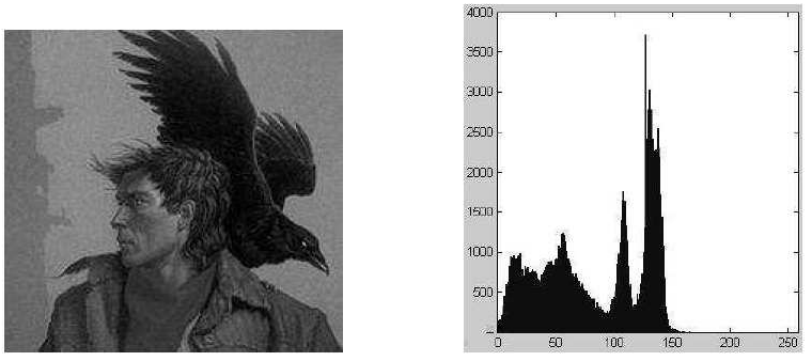


Figura 3.4: Exemplo de uma imagem e seu respectivo histograma (BARBOZA, 2005).

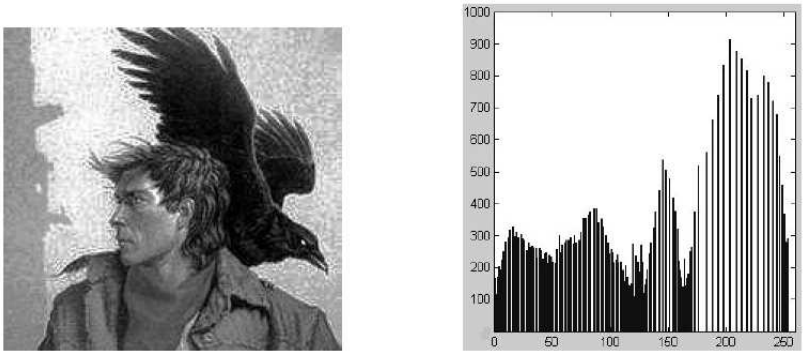


Figura 3.5: Exemplo de equalização de histograma. A imagem resultante e o histograma equalizado (BARBOZA, 2005).

Por fim, outras operações que merecem destaque no processamento de imagem são aquelas que realçam a imagem. Essas técnicas possuem objetivos variados, que dependem diretamente da aplicação em questão, mas em geram elas destacam uma determinada característica ou aspecto da imagem (GONZALEZ & WOODS, 2000 apud BARBOZA, 2004). O realce da imagem pode tanto atuar no domínio da freqüência quanto no domínio do espaço. A aplicação de filtros (passa-baixa ou passa-alta) são exemplos destas técnicas.

3.2 Processo de Reconhecimento de Identidade por Impressões Digitais

No capítulo anterior discutiu-se sobre a necessidade do ato de reconhecer a identidade na sociedade moderna. Também foi discutido sobre os meios de prova por posse, por conhecimento e por propriedade. Como último adendo a este assunto, é proposta uma classificação a respeito da forma de reconhecimento da identidade. Como visto na Figura 1.1, reconhecer consiste em responder uma das três perguntas. Essas perguntas diferem quanto a forma de prova disponível e a voluntariedade do indivíduo em ser reconhecido.

Quando há voluntariedade do indivíduo em ser reconhecido e este de antemão oferece alguma prova de identidade, o termo **Verificação** é o mais apropriado. Na mesma situação, porém sem dispor previamente de uma prova de identidade o termo mais correto é **Identificação**. Ambos podem ser classificados como uma forma de **Autenticação**. Já na **Investigação** não haveria vontade expressa por parte do indivíduo em ser reconhecido nem informação prévia sobre a sua identidade. A autenticação e a investigação são especializações do termo mais genérico *Reconhecimento*, conforme a Figura 3.6.

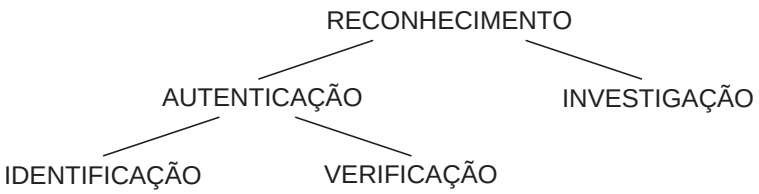


Figura 3.6: Classificação da formas de reconhecimento.

É útil fazer essa distinção, pelo fato de cada forma possuir as suas peculiari-

dades, e que no fim refletem no próprio processo de reconhecimento de identidade. Por exemplo, os sistemas de autenticação normalmente trabalham com o registro de duas digitais por indivíduo. Portanto, são incapazes de reconhecer a identidade a partir de uma ID latente. Situação essa coberta por sistemas de identificação civil, que no momento de registro capturam ID dos dez dedos das mãos e por toda a sua superfície (ID rolada).

Nas subseções seguintes são discorridas as etapas do Processo de Reconhecimento de Identidade por Impressões Digitais (PRIID). Este processo contém cinco etapas: Aquisição, Registro, Representação, Reconhecimento e Decisão (Ver Figura 3.7).

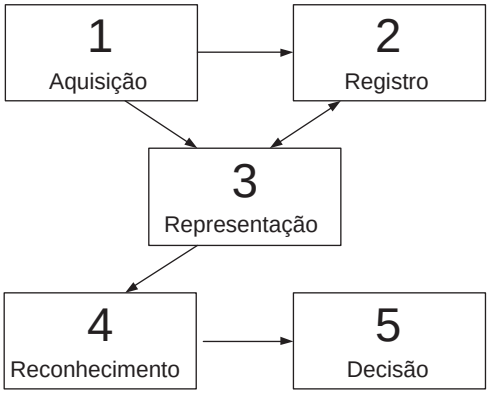


Figura 3.7: Etapas do processo de reconhecimento de identidade por impressões digitais.

3.2.1 Aquisição

A primeira etapa do PRIID é adquirir a ID. Qualquer insucesso ocorrido nesta etapa compromete por completo o PRIID. Os principais aspectos da etapa de Aquisição são: a forma, o meio, o modo de contato, o estado e a qualidade da ID, a qualidade da imagem obtida e a tecnologia do dispositivo de aquisição (Tabela 3.1).

Forma de Aquisição	Voluntária ou Involuntária
Meio de Aquisição	On-line ou Off-line
Modo de Contato	Batida, Rolada ou Arrastada
Estado e Qualidade da ID	Normal, Seca, Úmida, com Cortes, com Queimaduras etc ...
Qualidade da Imagem Obtida	Satisfatória ou Insatisfatória
Tecnologia do Dispositivo de Aquisição	Tinta *(ink-technique)*, Óticos *Solid-state*, Ultra-som e Outras

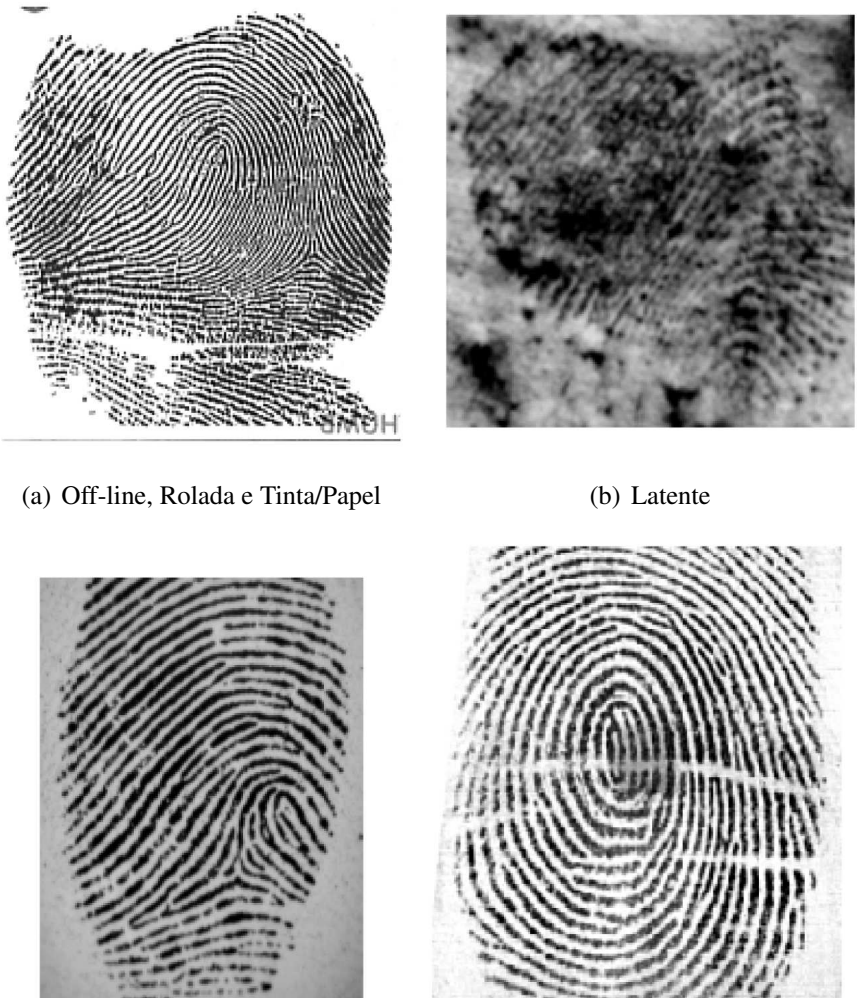
Tabela 3.1: Particularidades do processo de aquisição.

- Forma de Aquisição

Pode ser Voluntária ou Involuntária. Na primeira o individuo a ser reconhecido está presente e coopera com o procedimento de aquisição, na segunda forma ocorre o oposto. Vale ressaltar, que no primeiro caso pode haver aferição sobre a qualidade da imagem adquirida e repetição do procedimento, o que, em princípio, gera uma melhor aquisição da imagem da ID.

- Meio de Aquisição

Os meios de aquisição são: On-line e Off-line. A principal diferença entre o meio On-line e Off-line é que no primeiro a digitalização ocorre no mesmo momento da aquisição enquanto no segundo a digitalização é feita posteriormente. Latente é o vestígio de uma impressão digital em uma superfície qualquer.



(a) Off-line, Rolada e Tinta/Papel (b) Latente

(c) On-line, Batida e Ótico (d) On-line, Batida e Capacitivo

Figura 3.8: Exemplos de imagens de ID - meio de aquisição, modo de contato e dispositivo de aquisição (CHIKKERUR, 2005).

- Modo de Contato

É a maneira de contato entre a ID e o dispositivo de aquisição, pode ser do tipo Batido, Rolado ou Arrastado. Na aquisição do tipo Batido, a ID é pressionada verticalmente contra o dispositivo. No tipo Rolado, o contato inicia-se em uma lateral do dedo, passando depois pela região nuclear e terminando na outra lateral. Neste modo, quase toda a superfície da ID é capturada. No tipo Arrastado, o leitor da ID captura um pequena faixa da ID, devendo esta ser arrastada sobre o leitor afim de adquiri-la por completo. O modo está intrinsecamente relacionado com o dispositivo de aquisição.

- Estado e Qualidade da ID

O Estado e a Qualidade da ID dizem respeito às características momentâneas ou inerentes das ID. Por exemplo, a ID pode estar úmida ou seca ou pode conter ferimentos ou queimaduras. Todas essas características influenciam na qualidade do processo de Aquisição e no desempenho do processo de Reconhecimento.

- Qualidade da Imagem Capturada da ID

É o aspecto que trata sobre a qualidade da imagem fornecida pelo leitor da ID. É preciso atingir certo nível de qualidade, a fim de ser possível a extração de características (minúcias), e por conseqüência o reconhecimento. A qualidade é dependente de outros aspectos, ou seja, o estado e qualidade da ID, a resolução e o tamanho da área de captura do leitor, o modo de contato da ID, todos estes aspectos influenciam na qualidade da imagem a ser obtida.

- Dispositivos de Aquisição

É a técnica e o aparato envolvido na captura da imagem da ID. Podem ser On-line ou Off-line. A técnica mais tradicional de capturar a ID é a tinta/papel *(ink-technique)*. A tinta é passada na ID, e depois a ID é pressionada contra o papel. Outra forma de aquisição importante, principalmente no que tange questões policiais, é aquela que coleta os vestígios de uma ID. A esse tipo dá-se o nome de ID latente (RABELLO, 1996 apud KAZIENKO, 2003).

A coleta de ID latente envolve trabalho pericial e geralmente ocorre em locais de crime. A ID latente é produzida pelo contato dos dedos com determinadas superfícies. O próprio suor e a gordura dos dedos geram impressões digitais latentes. O processo de revelação de ID latente é dividido em três categorias de acordo com o tipo de reagente: método sólido, método líquido e método gasoso (SILVA, 2001 apud KAZIENKO, 2003).

A escolha do método varia de acordo com o tipo da superfície em que a ID latente está localizada.

Já nos casos de sistemas comerciais existem inúmeros dispositivos automáticos de aquisição, os *live-scan*. Praticamente, existem três categorias acerca da tecnologia empregada nestes equipamentos: ótico, *solid state* e ultra-som (MALTONI et al., 2003). A seguir, é feito um comentário sobre elas.

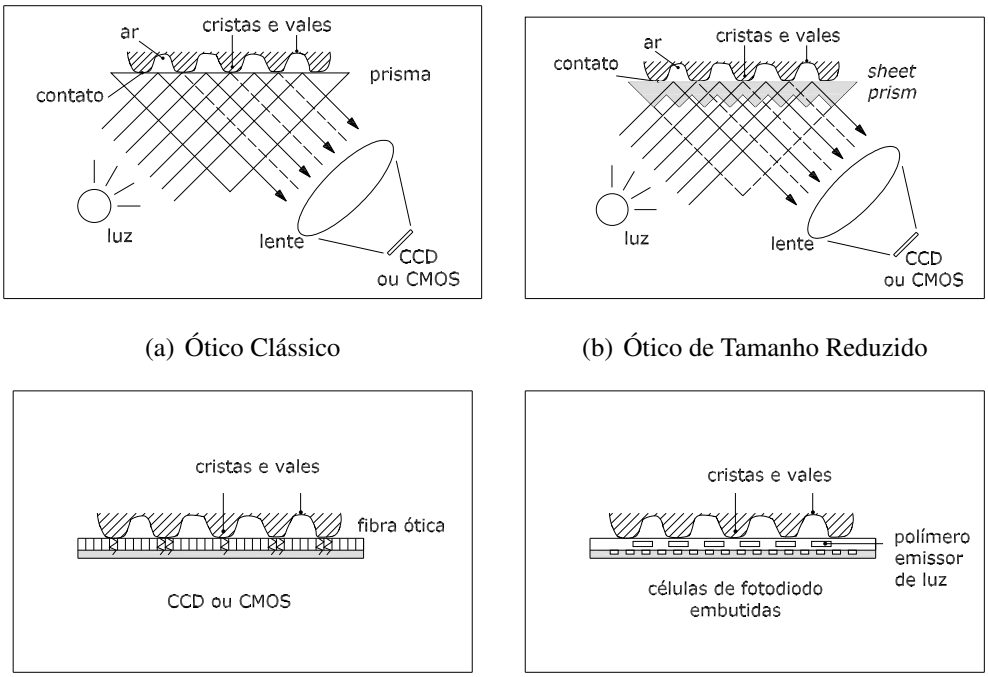
- Dispositivos Óticos

Os dispositivos óticos *(Optical sensors)* são baseados na tecnologia mais antiga e mais tradicional de leitores automáticos (On-line) de ID. A forma mais usual desta tecnologia consiste na emissão de luz em uma face do prisma, reflexão e absorção dessa luz pela ID e a captura da imagem refletida por um sensor CCD ou CMOS *(FTIR - Frustrated Total Internal Reflection)*. A Figura 3.9(a) mostra um dispositivo ótico clássico. É um dispositivo barato e que alcança boa precisão. Contudo, provoca distorção trapezoidal na imagem, tem a qualidade influenciada pelo estado da ID, deixa ruído das leituras anteriores e pode ser fraudado por uma ID falsa. Outro fato negativo é que devido ao tamanho do prisma há uma limitação de redução do tamanho do dispositivo em si (MALTONI et al., 2003) e (CHIKKERUR, 2005).

Um dispositivo de aquisição de tamanho reduzido se faz quase obrigatório pela existência de leitores embutidos em equipamentos como celular, mouse, teclado e etc. O leitor da Figura 3.9(b) tem o prisma formado por vários pequenos prismas *(sheet prism)* (Figura 3.9(b)), o que possibilita a redução do seu tamanho. Entretanto, a qualidade da imagem capturada é ligeiramente inferior ao leitor anterior (MALTONI et al., 2003).

Leitores de ID baseados em fibras-óticas também são de tamanho reduzido (Figura 3.9(c)). Neste sistema, as fibras-óticas transmitem as luzes residuais emitidas pela ID para o sensor CCD/CMOS. Nesta tecnologia, os sensores CCD/CMOS possuem o mesmo tamanho que a superfície de contato, o que provoca aumento no custo.

Por fim, outro dispositivo ótico importante é o eletro-ótico. Este leitor é constituído por duas camadas. A primeira contém um polímero que quando polarizado com certa voltagem emite luz de acordo com o potencial aplicado sobre a sua superfície. As cristas da ID tocam o polímero e os vales não. Desta forma, o potencial de luz emitido varia , permitindo que uma representação luminosa da impressão digital seja. A segunda



(a) Ótico Clássico (b) Ótico de Tamanho Reduzido

(c) Ótico Baseados em Fibras-óticas (d) Eletro-ótico

Figura 3.9: Dispositivos óticos de aquisição de ID (MALTONI et al., 2003).

camada, que está acoplada na parte inferior da primeira, é constituída de por células de fotodiodo embutidas que recebem a luz emitida pela primeira camada e a converte em uma imagem digital (Ver Figura 3.9(d)) (MALTONI et al., 2003).

- Dispositivos Solid-state

Os dipositivos do tipo *(Solid-state)*, também conhecidos como sensores de silício *(silicon sensors)*, foram patenteados na década de 80, não obstante só depois da metade da década de 90 é que eles começaram a serem comercializados (XIA & O'GORMAN, 2003 apud MALTONI et al, 2003). Esta tecnologia foi desenvolvida para ser produzir dispositivos de baixo custo e de pequeno tamanho. Os leitores desse tipo consistem numa matriz de *pixels* onde cada *pixel* é um próprio pequeno leitor. A ID entra diretamente em contato com a superfície de silício, não há componentes óticos nem sensores CCD/CMOS. A tecnologia envolvida para de converter o desenho da superfície da ID em sinais elétricos pode ser divida em quatro principais: a capacitiva, a térmica, a baseada no campo elétrico e a baseada no campo piezo elétrico.

O leitor capacitivo *(Solid-state Capacitive)* é composto por uma superfície retangular contendo várias placas micro-capacitoras (Figura 3.10). Essas microplacas agem

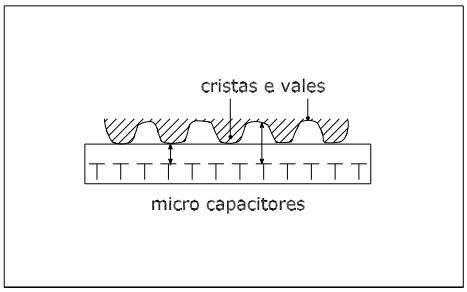


Figura 3.10: Aquisição *Solid-state* - Capacitivo (MALTONI et al., 2003)

como se fosse uma placa de um capacitor. As cristas e vales da ID agem como se fosse a outra placa dos micro-capacitores. A capacitância varia inversamente proporcional à distância entre as microplacas e a ID. As cristas da ID estão mais próximas das microplacas que os vales, assim, as diferenças de capacitâncias possibilitam a distinção das mesmas. Os leitores capacitivos são os de maior uso na atualidade (MALTONI et al., 2003).

Os leitores de ID baseados em sensores térmicos são feitos de materiais piro-elétricos *(pyro-eletric)*, ou seja, estes materiais mudam sua carga elétrica de acordo com a temperatura. É pela diferença da condução de calor entre o ar e as cristas da ID que este leitor consegue capturar a imagem da ID (MALTONI et al., 2003).

Os leitores baseados no campo elétrico consistem de um dispositivo que gera sinais senoidais e de uma matriz de antenas que recebem a transmissão desses sinais. A ID deve entrar em contato simultaneamente com o emissor e o receptor do sinal. A estrutura dérmica da ID modula este sinal, e a partir daí, se consegue construir a imagem da ID (MALTONI et al., 2003).

Os leitores baseados no campo piezo elétrico produzem um sinal elétrico quando uma força é aplicada sobre ele. A superfície de leitura é feita de um material não condutor que ao sofrer a pressão do dedo gera uma corrente elétrica. A intensidade da corrente gerada é proporcional a pressão aplicada, logo, como as cristas e os vales estão em distâncias diferentes, é possível construir a imagem da ID pela a diferença das intensidades das corrente (MALTONI et al., 2003).

- Dispositivos por Ultra-Som

Outra técnica importante utilizada é aquela que captura a imagem da ID por Ultra-som *(Ultrasound sensors)*. Esta tecnologia é provavelmente a que produz a imagem

como maior resolução (CHIKKERUR, 2005). O leitor de ID emite ondas ultra-sônicas e consegue medir a distância baseado na impedância da ID (linhas e vales), do ar e da placa de vidro (Figura 3.11). Existe no mercado dispositivos ultra-sônicos que alcançam a resolução de 1000dpi. Entretanto, esses tipos de leitores tendem a ser grandes e com várias partes móveis, o que acarreta dificuldade na operação.

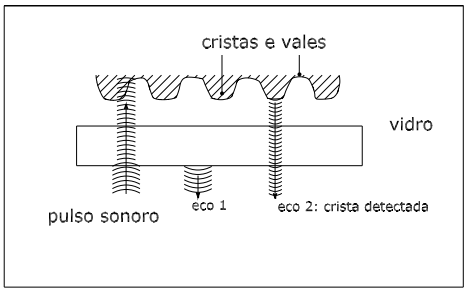


Figura 3.11: Aquisição por ultra-som (MALTONI et al., 2003)

3.2.2 Registro

A etapa de Registro é responsável pelo o armazenamento da representação *(template)* da ID e também pela consulta das representações de ID anteriormente registradas. O conteúdo armazenado está relacionado como a técnica adotada pelo PRIID. Ou seja, os métodos de reconhecimento baseado em minúcias só precisariam armazenar um vetor contendo o tipo, a posição e o ângulo de cada minúcia. Não havendo necessidade de armazenar a imagem capturada, evitando assim o consumo de espaço físico na unidade de armazenamento. Já outros métodos, como por exemplo, os baseados em correlação necessitam da imagem da ID, logo precisariam armazenar a imagem.

Entretanto, mesmo os sistemas baseados em minúcias podem utilizar outras informações, como por exemplo, as singularidades. Desta forma, a decisão sobre o que armazenar e como armazenar fica subordinado à estratégia do PRIID. É claro que sempre seria mais vantajoso armazenar a própria imagem, pois só assim o sistema PRIID estaria resguardado contra qualquer acusação acerca da veracidade do reconhecimento. Se o número de imagens a armazenar fosse pequeno não haveria problema algum. No entanto, uma estimativa feita por MALTONI et al (2003) mostra que caso fosse preciso armazenar todas imagens de ID de um registro civil o espaço necessário seria de aproximadamente 2000 terabytes. Ele chega a esse número considerando que cada imagem de ID digitali-

zada em 500dpi de resolução de 768×768 com 256 tons de cinza consumiria por volta de $590KB$. Levando em consideração que em registros civis são coletadas as ID de todos os dedos da mão, tanto da forma batida quanto rolada, espaço gasto chegaria a 10MB por indivíduo. Multiplicando os 10MB por uma população de 200 milhões alcançaria este valor de 2000 TB.

Cabe também a esta etapa proceder a busca eficiente das Representações candidatas ao reconhecimento positivo, para isso é esperado que exista alguma forma que agilize essa pesquisa. A classificação e indexação são meios que aceleram essa busca, eles estão descritos nas seções 3.2.4.1 e 3.2.4.2, respectivamente.

Outra questão importante presente nesta etapa é a estratégia de aquisição continuada. Mesmo que a ID seja uma característica permanente, é preferível que a ID seja capturada de tempos em tempos. Deste modo, qualquer alteração da ID será percebida pelo SB. Esta estratégia também faz com que a mesma ID seja adquirida em estados e posições diversas, fato esse pode aumentar a robustez do SB. Um técnica interessante consiste em justaposionar *(mosaicking)* várias imagens de uma ID (Ver Figura 3.12) com objetivo de formar uma imagem mais completa, por conseqüência com mais informações disponíveis (JAIN & ROSS, 2004) e (ULADAG et al., 2004).

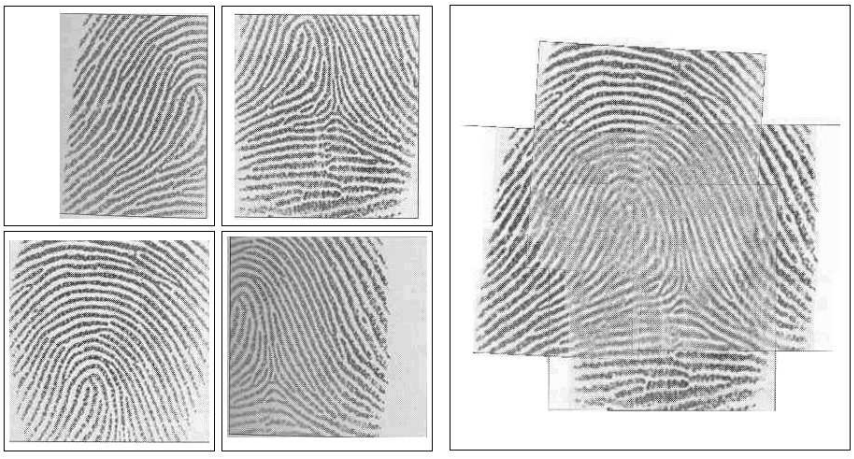


Figura 3.12: Justaposição *(mosaicking)* de quatro imagens da mesma impressão digital (MALTONI et al., 2003).

3.2.3 Representação

O principal objetivo da etapa de Representação é fornecer informações suficientes para que a etapa de Reconhecimento seja capaz de reconhecer a identidade do

indivíduo em questão. Para isso, cabe a etapa de Representação aplicar diversas técnicas, seja de aprimoramento da imagem ou de extração de características, com o único intuito de produzir uma representação fiel da ID adquirida. Esta etapa está fortemente relacionada com a abordagem empregada na etapa de reconhecimento.

Apesar das inúmeras abordagens de reconhecimento *(matching*) de ID, elas podem ser classificadas em três categorias: o reconhecimento baseado na correlação da imagem da ID *(Correlation-based matching)*, o reconhecimento baseado nas minúcias da ID *(Minutiae-based matching)* e o reconhecimento baseado nas características gerais da ID *(Ridge feature-based matching)* (MALTONI et al., 2003). Portanto, o alvo da etapa de Representação é garantir uma extração correta das características da ID, para isso pode ser necessário ações que elimine o ruído ou facilite a extração. A Figura 3.13 apresenta as sub-etapas de Representação.

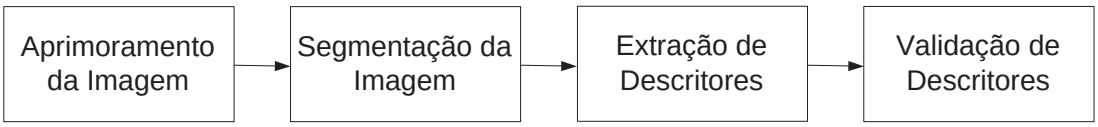


Figura 3.13: Subetapas de etapa de representação: aprimoramento da imagem, segmentação da imagem, extração de descritores e validação de descritores.

A imagem da ID é suscetível a diversos níveis de qualidade (Ver Figura 3.14). Geralmente, a má qualidade é ocasionada por ruído gerado no processo de coleta ou pela própria condição da ID (cortes ou queimaduras).

Figura 3.14: Exemplos de imagens de ID com diferentes níveis de qualidade. Da esquerda para direita a qualidade diminui. A primeira possui um bom contraste entre as linhas e o vales, na segunda há linhas com espessuras diversas, a terceira é um ID seca e na última há muitas falhas (CHIKKERUR, 2005).

O aprimoramento vem na tentativa melhor a qualidade da imagem e de reduzir os ruídos presentes na ID. Inúmeros estudos acerca de aprimoramento já forma realizados, como o de Hong, Wan & Jain (1998, apud MALTONI et al., 2003) que propuseram uma normalização definida pela Equação 3.5, onde m e v são, respectivamente, a média e a variância, e v_0 é a variância desejada e m_0 é a média desejada. Outros trabalhos, como o de Marques (2004), propuseram a manipulação do histograma (Ver Figura 3.15), a ampliação de contraste *(contrast stretchin)* e a aplicação do filtro de Wiener (GREENBERG et al., 2000 apud MALTONI el.,2003). No entanto, mesmo melhorando o contraste da imagem esses métodos são incapazes de separar linhas unidas ou preencher vazios de uma imagem de má qualidade.

$$I'[x,y] = \begin{cases} m_0 + \sqrt{(I[x,y]-m)^2.v_0/v} & \text{se } I[i,j] > m \\ m_0 - \sqrt{(I[x,y]-m)^2.v_0/v} & \text{caso contrário} \end{cases} \tag{3.5}$$

(a) Imagem Bruta (b) Imagem Equalizada

Figura 3.15: A esquerda uma imagem bruta de uma ID e a direita a imagem após a equalização de histograma.

Já o trabalho de Oliveira & Leite (1997) corrige eventuais falhas (ex. cortes) da ID através de operações morfológicas. A Figura 3.16 mostra a imagem de uma ID com cortes e após operações morfológicas as linhas da ID são conectadas. Já Ko (2000) apresenta algumas técnicas de aprimoramento baseado no espectro da imagem.

Um filtro de grande uso no aprimoramento da imagem de ID é o filtro de Gabor. Este filtro serve tanto para melhorar o contraste entre as linhas e vales quanto para eliminar ruídos. A grande aplicabilidade deste filtro se deve ao fato dele realçar a qualidade de imagens senoidais, o que serve muito bem para as imagens de ID, pois a

Figura 3.16: A primeira imagem mostra um ID com cortes, na segunda imagem são localizados os cortes da ID e na terceira imagem as linhas da ID são conectadas (OLIVEIRA & LEITE, 1997).

sinuosidade das cristas e vales da ID faz com que os tons de cinza da imagem ID variem como se fossem uma senóide. No trabalho de Marques (2004) há uma descrição detalhada sobre o funcionamento do filtro de Gabor, inclusive com uma proposta de uma rede neural que implementa um filtro de Gabor. A Figura 3.17 ilustra a imagem de uma ID antes e depois da aplicação do filtro de Gabor.

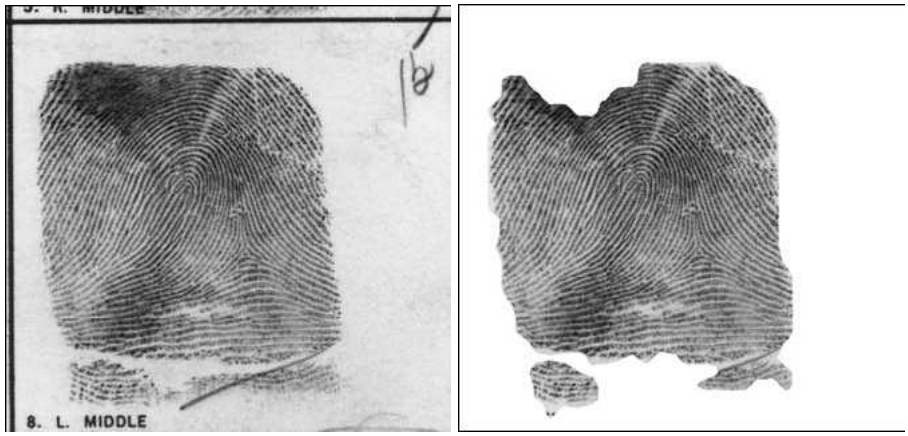
(a) Imagem Bruta (b) Filtro de Gabor

Figura 3.17: A melhoria da qualidade da imagem após a aplicação do filtro de Gabor proposto por Marques (2004).

A segmentação é a etapa seguinte ao aprimoramento, nesta etapa é realizada a localização da região de interesse. A Figura 3.17(b) ilustra só a região que contém a ID, ou seja, a segmentação excluí da imagem a região que não faz parte da ID. Marques & Thomé (MARQUES & THOMÉ, 2005) construíram uma método de segmentação usando redes neurais. Neste caso, as redes neurais recebem como entrada o espectro de freqüência de uma região da imagem da ID e determinam se a região faz parte ou não da ID. A segmentação é extremamente útil quando as imagens da ID são retiradas de registros

públicos (Ver Figura 3.18).

Depois da segmentação vem a extração de descritores ou características. Esta é a principal parte do processo de representação. É nesta que ocorre de fato a extração de informações que serão usadas no reconhecimento. Os descritores mais usados são as mesmas características comentadas na Seção 2.2.2, ou seja, as minúcias, as singularidades, o caminho das linhas da ID, o número de linhas entre dois pontos da ID, a espessura das linhas e a própria imagem. Além dessas, acrescenta-se o campo direcional e freqüência de linhas de ID como descritores. Nas subseções seguintes são descritas algumas técnicas de extração de características, com maior foco na obtenção do campo direcional, extração de singularidades e de minúcias.



(a) Imagem Bruta (b) Imagem Após Segmentação

Figura 3.18: A segmentação exclui as regiões da imagem que não fazem parte da ID (MARQUES, 2004).

3.2.3.1 Construção do Campo Direcional

O campo direcional[1] é uma forma de descrever a ID através das inclinações predominantes das suas linhas em uma pequena região. Com a informação relativa a essas inclinações consegue-se ter uma idéia do desenho da ID (Ver Figura 3.19). O campo direcional pode ser definido da seguinte forma: seja I uma imagem qualquer, dividi-se I em pequenas regiões sendo p o ponto central desta região. A inclinação θ_{xy} de uma região será igual ao ângulo que a linha ou vale que passa pelo ponto p faz com o eixo horizontal. Como a direção da linha ou vale de uma ID não possui sentido, θ_{xy} assume valores entre

[1]Também chamando de imagem direcional.

$[0..180^o[$. Geralmente a região é de tamanho ímpar de modo que o seu centro coincida com um *pixel*. O campo direcional (I_{md}) será o conjunto de inclinações (θ_{xy}) de toda a imagem.

Na determinação do campo direcional, a inclinação θ_{xy} é calculada somente para cada região escolhida, e não para todos os *pixels*. Portanto, em uma imagem I de (270×270) utilizando uma máscara (região) (9×9), o cálculo da inclinação θ_{xy} é efetuado 900 vezes. Logo, se o campo direcional contiver apenas 8 direções distintas $\{0, \frac{\pi}{8}, \frac{\pi}{4}, \frac{3\pi}{8}, \frac{\pi}{2}, \frac{5\pi}{8}, \frac{3\pi}{4}, \frac{7\pi}{8}\}$ seriam necessários somente 3 bits para armazenar cada direção. Por conseqüência, nesta mesma imagem I com dimensões 270×270 em tons de cinza ocuparia o espaço de pelo menos 72Kb, enquanto o campo direcional ocuparia menos de 450 *bytes*. Em suma, o campo direcional consegue representar o desenho da ID e exige pouco espaço físico.

(a) Imagem Bruta (b) Campo Direcional

Figura 3.19: Exemplo de um campo direcional com uma região 9×9 com 8 direções.

A abordagem mais natural para determinar a inclinação θ_{xy} seria a baseada no cálculo do gradiente da imagem da ID (MALTONI et al., 2003). O gradiente $\nabla(x_i, y_j)$ no ponto (x_i, y_j) de uma imagem I é um vetor bidimensional $[\nabla_x(x_i, y_j), \nabla_y(x_i, y_j)]$ onde os componentes ∇_x e ∇_y são derivadas da imagem I na posição (x_i, y_i) em relação ao eixo x e ao eixo y, respectivamente. O gradiente indica a direção da maior mudança da intensidade. Logo, a direção da inclinação θ_{xy} do campo direcional seria ortonormal a direção dada pelo gradiente. O cálculo do gradiente pode ser feito pela aplicação do operador de *Prewitt* ou de *Sobel* e a determinação da inclinação θ_{xy} pode ser obtido pela função arco tangente da razão ∇_y/∇_x. No trabalho de Lima (2002) há uma descrição minuciosa do algoritmo de construção do campo direcional baseado no cálculo do gradiente. Entretanto, devido a descontinuidade da função $tan(x)$ quando x está próximo de $\pi/2$ e por ser sensível a

ruído, a determinação da campo direcional pelo o gradiente possui algumas desvantagens (MALTONI et al., 2003).

Outro fato negativo na construção do campo direcional pelo cálculo do gradiente apontado por Maltoni et al. (2003) é que não se pode estimar a inclinação θ_{xy} baseada nas médias das direções resultante do cálculo do gradiente. Por exemplo, se a inclinação fosse a média dos ângulos de 5º e 175º resultaria no valor igual a 90º, entretanto a inclinação certa deveria se igual 0º. Para eliminar o problema da circularidade dos ângulos Kass & Witkin (1987 apud MALTONI et al., 2003) propuseram um método simples que permite o cálculo da inclinação θ_{xy} pela média dos gradiente. Para isso, eles duplicaram os ângulos. Outros trabalhos, como os de Rao (1990 apud MALTONI et al, 2003), Ratha, Chen & Jain (1995, apud MALTONI et al, 2003) e Bazez & Gerez (2002b apud MALTONI et al, 2003), seguem a mesma idéia.

Implementou-se neste trabalho o método de construção proposto por Karu et al. (1996, apud COSTA, 2001). A escolha deste método se deve ao fato dele ser simples e de baixo custo computacional. Entretanto, um aspecto negativo deste método é que ele trabalha somente com 8 direções possíveis. Mesmo assim, é o suficiente para ser utilizado no processo de extração de singularidade pelo índice de Poincaré.

O método Karu et al. (1996, apud COSTA, 2001) determina o campo direcional de uma ID da seguinte forma:

1. Dividi-se a imagem da ID em regiões (máscaras) não sobrepostas de dimensão igual a 9×9 ou 17×17, caso a dimensão da imagem não seja múltiplo de 9 ou 17 as regiões limítrofes da imagem são descartadas;

2. Sobre cada região calcula-se os valores de $S_0, S_1, ..., S_7$ de acordo com as equações 3.6 a 3.13, sendo que $I(i, j)$ indica a luminância do *pixel* na posição (i, j) da imagem da ID. Os valores $S_{0..7}$ indicam o somatório dos tons de cinza nas direções de $\{0, \frac{\pi}{8}, \frac{\pi}{4}, \frac{3\pi}{8}, \frac{\pi}{2}, \frac{5\pi}{8}, \frac{3\pi}{4}, \frac{7\pi}{8}\}$ como mostrado na Figura 3.20;

$$S_0 = \sum_{k=-2}^{2} I(i, j+2k) - I(i, j) \tag{3.6}$$

$$S_1 = \sum_{k=-2}^{2} I(i, j-2k) - I(i, j) \tag{3.7}$$

$$S_2 = \sum_{k=-2}^{2} I(i+2k, j-2k) - I(i,j) \tag{3.8}$$

$$S_3 = \sum_{k=-2}^{2} I(i+2k, j-k) - I(i,j) \tag{3.9}$$

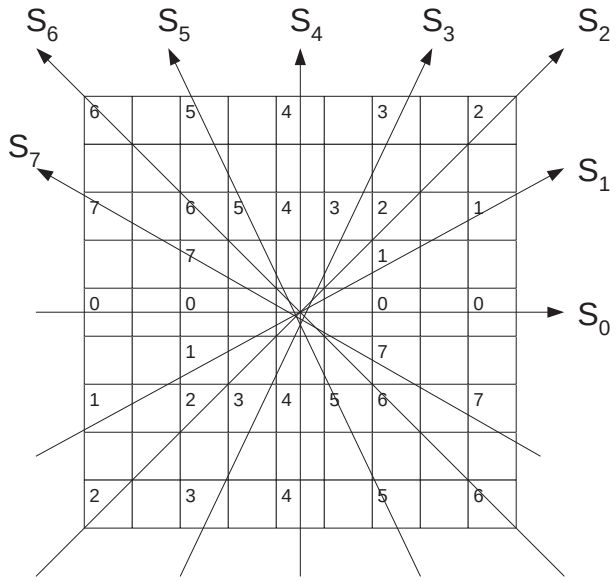


Figura 3.20: A máscara 9×9 usada para calcular a campo direcional (COSTA, 2001).

$$S_4 = \sum_{k=-2}^{2} I(i+2k, j) - I(i,j) \tag{3.10}$$

$$S_5 = \sum_{k=-2}^{2} I(i+2k, j+k) - I(i,j) \tag{3.11}$$

$$S_6 = \sum_{k=-2}^{2} I(i+2k, j+2k) - I(i,j) \tag{3.12}$$

$$S_7 = \sum_{k=-2}^{2} I(i+2k, j-k) - I(i,j) \tag{3.13}$$

3. Atribua a S_p o menor valor entre $S_{0..7}$ e a S_q o maior valor $S_{0..7}$;

4. A orientação D predominante na região em questão é dada pela Equação 3.14. Que na verdade quer dizer que caso o *pixel* central tenha uma intensidade baixa a inclinação predominante será igual a direção $(S_0...S_7)$ que possui menor intensidade e caso o *pixel* central tenha uma intensidade alta a inclinação predominante será igual a direção $(S_0...S_7)$ que possui maior intensidade.

$$D \begin{cases} p & \text{se } (4I(i,j) + S_p + S_q) < \frac{3}{8} \sum_{i=0..7} S_i \\ q & \text{caso contrário} \end{cases} \tag{3.14}$$

A Figura 3.21 ilustra exemplos do campo direcional construído pelo método anterior a partir da imagem bruta e da imagem após a aplicação do filtro de Gabor. Nestas figuras percebem-se algumas inclinações que são heterogêneas em relação aos seus vizinhos. Para corrigir essas situações, Costa (2001) propôs um método de suavização baseado na medida estatística *moda*, que é definido da seguinte forma:

1. Para todas as inclinações θ_{ij} do campo direcional, calcule a *moda* entre os elementos vizinhos-de-8 da inclinação θ_{ij} mais a própria inclinação θ_{ij} em questão;

2. Selecione a inclinação θ_{xy} retornada pela *moda*. Caso haja empate, entre as inclinações empatadas selecione a que for igual a θ_{ij} ou a de menor valor;

3. Armazene a inclinação em um campo direcional temporário;

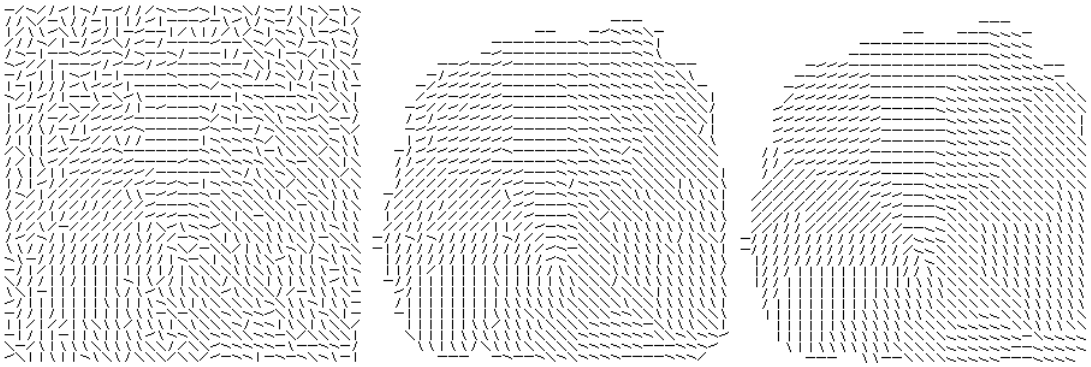
4. Finalizado o percurso de todas as inclinações, atribua os valores do campo direcional temporário ao campo direcional original;

A Figura 3.21(c) mostra um campo direcional após a suavização proposta por Costa (2001).

3.2.3.2 Extração de Singularidades

-Pelo Índice de Poincaré

Depois de construído o campo direcional é possível a determinação das singularidades. O primeiro método implementado é baseado no Índice de Poincaré que foi proposto por Kawagoe e Tojo (1984, apud MALTONI, 2003). Este pode ser descrito da seguinte forma: seja G uma campo vetorial e C uma curva imersa em G, o índice de Poincaré $P_{G,C}$ é definido como a rotação total dos vetores de G sobre a curva C (Ver Figura 3.22).



(a) Campo Direcional - Bruta (b) Campo Direcional - Gabor (c) Campo Direcional - Suavizado

Figura 3.21: Exemplos de um campo direcional construídos a partir da imagem Bruta, da imagem após o filtro de Gabor, da imagem após o filtro de Gabor e suavizado.

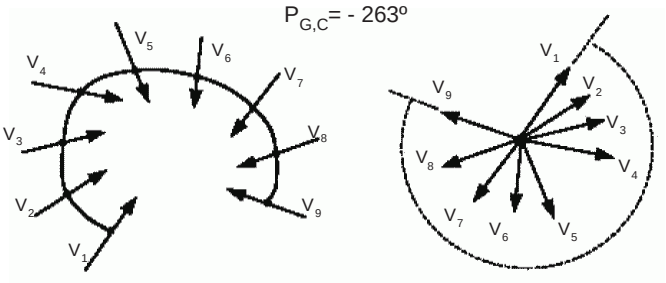


Figura 3.22: Índice de Poincaré calculado sobre um curva C imersa em um campo vetorial G.

No contexto deste trabalho, o índice de Poincaré determina, a partir do campo direcional D, se em uma região há uma singularidade ou não. Considera-se o campo direcional como se fosse o campo vetorial G e a região $[i, j]$ do campo direcional o ponto onde a rotação total do vetores é calculada. O índice de Poincaré $P_{G,C}$ na região $[i, j]$ é calculado da seguinte forma (MALTONI et al., 2003):

- A curva C é definida pelos elementos ordenados de D em torno da inclinação $[i, j]$ do campo direcional;

- O índice de Poincaré $P_{G,C}(i, j)$ é calculado somando-se as diferenças entre os elementos adjacentes da inclinação $[i, j]$ do campo direcional (Equação 3.15). Escolhe-se qualquer sentido (horário ou anti-horário). Caso seja escolhido o sentido horário, a soma das diferenças dos elementos adjacentes ficaria conforme a Equação 3.16. O índice de Poincaré assume somente valores discretos como: 0^o, 180^o e 360^o. A

associação entre os valores do índice de Poincaré e os tipos de singularidade está descrita na Equação 3.17.

$$P_{G,C}(i,j) = \sum_{k=0..7} angulo(d_k, d_{(k+1)mod8}) \tag{3.15}$$

$$\begin{aligned} P_{G,C}(i,j) &= (d_0 - d_1) + (d_1 - d_2) + (d_2 - d_3) + (d_3 - d_4) + \\ &\quad (d_4 - d_5) + (d_5 - d_6) + (d_6 - d_7) + (d_7 - d_0) \end{aligned} \tag{3.16}$$

$$P_{GC}[i,j] \begin{cases} 0^o & \text{se } [i,j] \text{ não pertence a nenhuma região singular} \\ 360^o & \text{se } [i,j] \text{ pertence a uma região Espiral (Whorl)} \\ 180^o & \text{se } [i,j] \text{ pertence a uma região com singularidade Núcleo (ápice)} \\ -180^o & \text{se } [i,j] \text{ pertence a uma região com singularidade Delta} \end{cases} \tag{3.17}$$

Desta forma, a partir dos valores das inclinações do campo direcional é calculado o índice de Poincaré. A Figura 3.23 mostra exemplos hipotéticos do cálculo do índice de Poincaré, nota-se que a vizinhança de uma inclinação do campo direcional $[i,j]$ é formados por 8(oito) inclinações $d_k(0 \leq k \leq 7)$. A Figura 3.24 mostra um exemplo real da extração de singularidade do tipo Núcleo pelo índice de Poincaré.

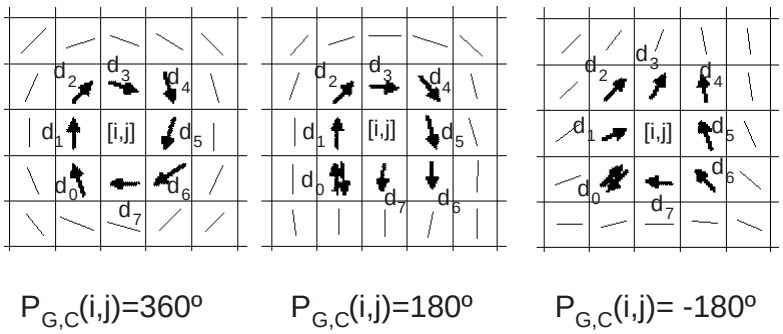


Figura 3.23: Exemplo do cálculo do índice de Poincaré - na imagem da esquerda $P_{G,C}(i,j) = 360^o$ portanto é uma singularidade do tipo Whorl, na imagem do centro $P_{G,C}(i,j) = 180^o$ portanto é uma singularidade do tipo Núcleo e imagem da direita $P_{G,C}(i,j) = -180^o$ portanto é uma singularidade do tipo Delta.

Há muitos trabalhos na literatura científica que emprega o índice de Poincaré como método de extração de singularidades. Cada trabalho emprega uma determinada particularidade e também utiliza uma forma específica de construção do campo direcional, outros aplicam um pós-processamento a fim de eliminar falsas detecções. Por fim, o método de índice de Poincaré se mostra como uma técnica satisfatória, principalmente se aplicadas a imagens de boa qualidade. No Capítulo 4 na seção 4.4.1.1 é apresentado os resultados obtidos da extração de singularidades pelo método do índice de Poincaré submetidos sobre o banco DB1 do FVC 2000.

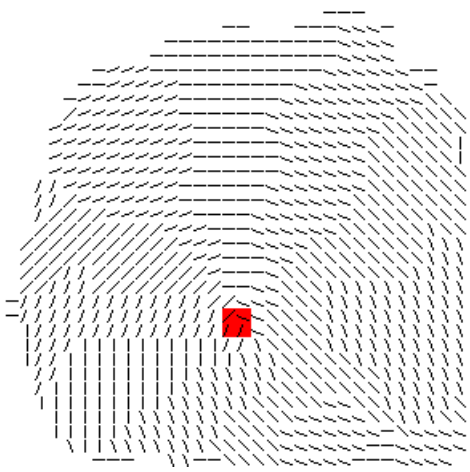


Figura 3.24: Exemplo de detecção de singularidade do tipo Núcleo pelo índice de Poincaré.

-Proposto por Jain et al. (JAIN et al., 2000)

Em seu artigo, Jain et al. (JAIN et al., 2000) afirma que os métodos de extração de singularidades baseados no campo direcional ou índice de Poincaré atingem bons resultados somente quando aplicados em imagens de boa qualidade. Por conseqüência, em ID que possuam cortes ou queimaduras esses métodos não alcançam bom desempenho. Desta forma, Jain et al (2000) propõe um método de localização da singularidade do tipo Núcleo (*Reference Point Location*).

Neste trabalho, os autores afirmam que para um algoritmo de detecção atingir um bom desempenho em imagens de má qualidade uma grande região da ID deve ser analisada. Por outro lado, uma detecção com alta precisão deve ser capaz de perceber pequena variações em uma região pequena da ID. O método proposto por Jain et al (2000) vem de encontro a este problema, para isso a determinação da singularidade é baseada em

uma análise de múltipla resolução do campo direcional. O método proposto é composto de 7 passos conforme a seguir.

1. É construído um campo direcional D com regiões (máscaras) de dimensão $w \times w$;

2. O campo direcional D é suavizado (filtro de passa-baixa), para isso é preciso transformar o campo direcional em um vetor contínuo Φ. Essa transformação é dada pelas equações 3.18 e 3.19. Sobre este vetor resultante é aplicado o filtro de passa-baixa de acordo como as equações 3.20 e 3.21 onde W é um filtro de dimensão $w_\Phi \times w_\Phi$. A inclinação do campo direcional resultante é dada pela equação 3.22.

$$\Phi_x(i,j) = cos(2D(i,j)) \tag{3.18}$$

$$\Phi_y(i,j) = sen(2D(i,j)) \tag{3.19}$$

$$\Phi'_x(i,j) = \sum_{u=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} \sum_{v=\frac{-w_\Phi}{2}}^{\frac{w_\Phi}{2}} W(u,v).\Phi_x(i-uw, j-vw) \tag{3.20}$$

$$\Phi'_y(i,j) = \sum_{u=-\frac{w_\Phi}{2}}^{\frac{w_\Phi}{2}} \sum_{v=\frac{-w_\Phi}{2}}^{\frac{w_\Phi}{2}} W(u,v).\Phi_y(i-uw, j-vw) \tag{3.21}$$

$$D(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right) \tag{3.22}$$

3. É calculado ε, uma imagem contendo somente a componente *seno* do campo direcional D' de acordo com a Equação 3.23 (Veja Figura 3.26(c));

$$\varepsilon(i,j) = sen(D'(i,j)) \tag{3.23}$$

4. Uma imagem A é criada para ser usada na indicação do ponto singular;

5. Para cada *pixel* (i,j) de ε, integre a intensidade do *pixel* em questão nas regiões R_I e R_{II} como mostrado na Figura 3.25 e atribua ao *pixel* correspondente na imagem A o valor da diferença dada pela Equação 3.24. As regiões R_I e R_{II} são determinadas empiricamente através de testes sobre um grande base de imagens de ID e suas

formas geométricas são desenhadas para capturar a curvatura máxima da linhas da ID.

$$A(i,j) = \sum R_I \varepsilon(i,j) - \sum R_{II} \varepsilon(i,j) \tag{3.24}$$

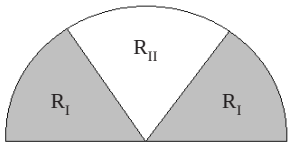
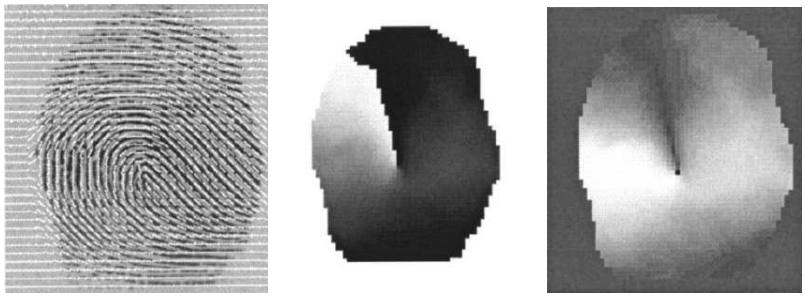


Figura 3.25: Regiões I e II utilizado na integração ε intensidade de *pixels* para $A(i,j)$.

6. Encontre o valor máximo de A e atribua sua coordenada a coordenada do ponto singular;

7. Repita n vezes os passos 1 a 6 , sendo em cada iteração altere o tamanho da região (máscara) para $w' \times w'$ onde $w' < w$ e restrinja a busca do ponto singular na região onde o mesmo for detectado na iteração anterior. Nos experimentos testados pelo autor do artigo foi realizado 3 iterações sendo $w = 15, 10\ e\ 5$.



(a) Imagem (a) (b) Imagem (b) (c) Imagem (c)

Figura 3.26: Extração da singularidade proposta por Jain et al. (2000). A Imagem (a) mostra o campo direcional suavizado sobreposto sobre a imagem da ID, a imagem (b) mostra a distribuição da intensidade do campo direcional e a imagem (c) o componente seno campo direcional, o ponto mais escuro é a posição do ponto singular (JAIN et al., 2000).

A idéia de multi-resolução proposta por Jain et al. (2002) é confirmada na iteração com as mudanças do valor de w. Este método foi implementado com o auxílio de

bibliotecas já disponibilizadas no site da ferramenta MATLAB [2]. A Figura 3.27 mostra os resultados da implementação deste método.

(a) Sobre a imagem bruta (b) Sobre a imagem após o filtro de Gabor

Figura 3.27: Exemplos do extração de singularidade pelo método proposto por Jain et al. (2002).

3.2.3.3 Extração de Minúcias

A maioria dos SB baseados em ID utiliza minúcias como características identificadoras. Por esta razão, o processo de extração de minúcias é uma tarefa vital ao PRIID. A literatura científica apresenta várias técnicas acerca deste assunto, no entanto, a maioria das técnicas trabalha em cima da imagem limiarizada (binarizada) conforme ilustrado pelo esquema da Figura 3.28. Este esquema retrata o processo de obtenção de minúcias clássico e foi o implementado neste trabalho. Nos parágrafos seguintes é exposta cada uma dessas subetapas.

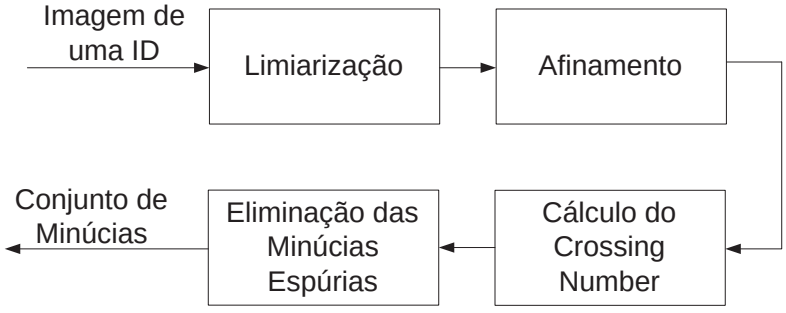


Figura 3.28: Etapas do processo de extração de minúcias.

A primeira etapa corresponde a limiarização (binarização) da imagem da ID,

[2]http://www.mathworks.com/matlabcentral/fileexchange/

ou seja, transformar a imagem em tons de cinza para preto & branco. A limiarização pode produzir algumas situações não desejadas como, por exemplo, a divisão de uma linha em duas ou a junção de duas linhas. Um exemplo dessa situação está retratada na Figura 3.29. Na Figura 3.29(b) é feita uma limiarização global, isto é, calcula-se a intensidade média (I_{media}) de todos *pixels* da imagem e depois altera-se todos os *pixels* de acordo com a Equação 3.25. Na Figura 3.29(c) é feito o mesmo processo, no entanto (I_{media}) é intensidade média de uma região em torno do *pixel*. Nota-se que na primeira figura existe uma junção de duas linhas, já na segunda estas linhas permaneceram isoladas. Moayer & Fu (1986 apud MALTONI et al., 2003) e Verma, Majumdar & Chatterjee (1987 apud Maltoni et al., 2003) conceberam adaptações a limiarização com o intuito de evitar esses tipos de problemas. Neste trabalho, optou-se por implementar a limiarização local.

(a) Imagem após filtro de Gabor (b) Limiarização global (c) Limiarização local

Figura 3.29: Problemas que podem ocorrer na limiarização (binarização). Na Figura (b) uma linha é erroneamente conectada a outra, o que não ocorre na Figura (c).

$$I'[i,j] \begin{cases} 0 & \text{se } I[i,j] \leq I_{media} \\ 1 & \text{se } I[i,j] > I_{media} \end{cases} \tag{3.25}$$

Após realizada a limiarização aplica-se o afinamento (esqueletização) da imagem para depois localizar as prováveis posições das minúcias. As técnicas de afinamento *(thinning)* são usadas em diversas aplicações, como por exemplo, de reconhecimento de caracteres, de análise de documentos e outras aplicações gráficas. Entre os métodos de afinamento para ID, Maltoni et al. (2003) destaca o algoritmo de Arcelli & Baja (1984 apud MALTONI et al., 2003) e de Ratha, Chen and Jain (1995 apud MALTONI et. al, 2003). O afinamento utilizado neste trabalho é o da biblioteca da ferramenta MATLAB, este utilizada os trabalhos de LAM (1992) como referência. A Figura 3.30 mostra o resultado do processo de afinamento aplicado na imagem bruta e na imagem após o filtro de Gabor. Fica claro que no afinamento da Figura 3.30(a) a detecção de minúcias teria um

desempenho muito ruim se comparado como o afinamento da Figura 3.30(b).

(a) Afinamento da Imagem Bruta (b) Afinamento da Imagem Gabor

Figura 3.30: Exemplo de afinamento sobre a imagem bruta e sobre a imagem após a aplicação do filtro de Gabor.

Obtida a imagem afinada, inicia-se o processo de localização das minúcias. Para todos os *pixels* da imagem é calculado o seu *crossing number* (Ver Equação 3.26) (ARCELLI & BAJA, 1984 apud MALTONI et al., 2003). O *crossing number* $cn(p)$ do *pixel* p numa imagem afinada é definido como a metade da soma da diferenças entre de dois *pixels* adjacentes em uma vizinhança-de-8 de p onde p_0,p_1,...,p_7 são os *pixels* vizinhos-de-8 em um seqüência ordenada e $val(p) \in \{0,1\}$ (Ver Equação 3.26).

$$cn(p) = \frac{1}{2} \sum_{i=1..8} |val(p_{i \bmod 8}) - val(p_{i-1})| \tag{3.26}$$

Pelo valor do *crossing number* tem-se uma estimativa se o *pixel* em questão indica uma minúcia ou não. A Tabela 3.2 mostra a associação entre o valor do *crossing number* e o seu significado. Por exemplo, $cn(p) = 1$ indica uma terminação e a $cn(p) = 3$ uma bifurcação (Ver Figura 3.31).

Tabela 3.2: Significado do valor *crossing number*

Crossing Number	Significado
0	Ponto Isolado
1	Terminação (Fim-de-Linha)
2	Ponto Contínuo da Linha
3	Bifurcação
4	Cruzamento

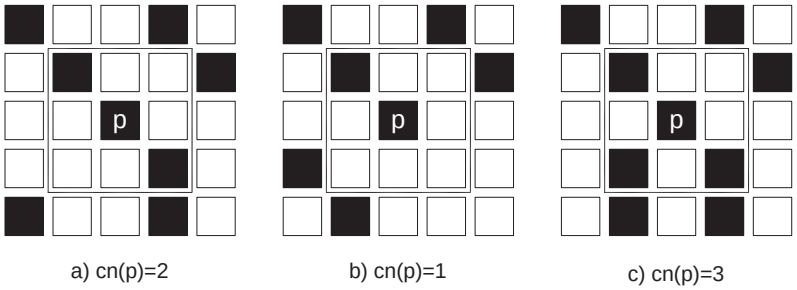
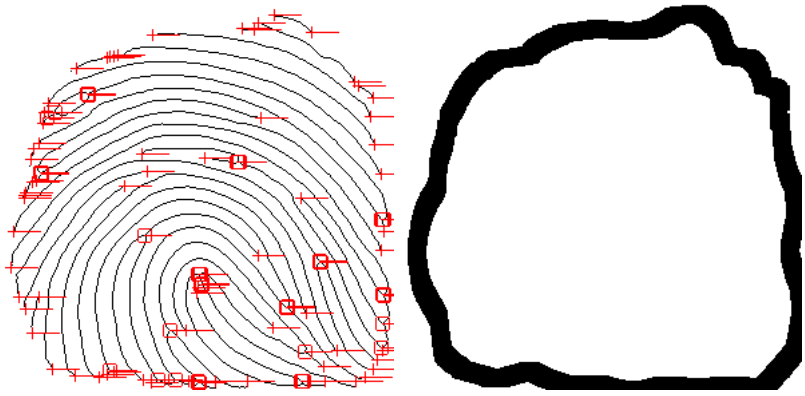


Figura 3.31: Associação do Valor do *crossing number* com o Tipo de Minúcia. a) um pixel dentro da linha; b) um pixel no fim-de-linha c) um pixel na bifurcação da linha.

Feita uma análise sobre o cálculo do *crossing number* aplicado na imagem afinada percebe-se que os *pixels* no final das linhas próximos da borda da ID teriam $cn(p) = 1$, contudo esses pontos não são minúcias. Para resolver isso, é feito um pós-processamento que elimina as minúcias espúrias. No método de extração implementado, todas as minúcias próximas da borda ou próximas de outras minúcias são classificadas como espúrias, e, portanto não são utilizadas na verificação. A razão de se eliminar minúcias próximas entre si é justificada pelo fato de que qualquer ruído existente na imagem geraria um pequeno segmento na imagem afinada, e assim, os pontos nas extremidades deste segmento teriam $cn(p) = 1$. O trabalho de Farina & Kovacs-Vajna (1999) discute várias técnicas que evitam extrair falsas minúcias de uma imagem afinada. A Figura 3.32 ilustra o processo de eliminação de falsas minúcias.

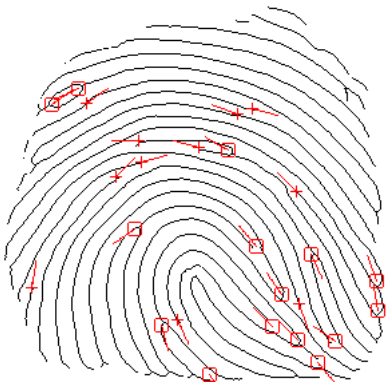
Durante os testes do processo de localização de minúcias foi constatado que há muitos casos de *pixels* próximos a uma bifurcação que retornam o *crossing number* igual a 3 (três) (Ver Figura 3.33). Estes *pixels* de $cn(p) = 3$ próximos entre si seriam excluídos no processo de eliminação de minúcias espúrias. Preferiu-se buscar as bifurcações através da localização de terminações na imagem negativa. Isto é possível devido a propriedade de uma bifurcação virar uma terminação na imagem negativa, como visto na Seção 2.2.2.2. A Figura 3.34 ilustra uma imagem de ID e sua respectiva imagem negativa com fundo branco. Além disso, é bem mais fácil calcular o ângulo de uma minúcia do tipo terminação do que o de uma bifurcação. Desta forma, a posição da bifurcação é a mesma que a posição da terminação em uma imagem negativa e o ângulo da bifurcação é o ângulo da terminação mais 180^o.

O próximo passo após a localização das posições das minúcias, é a determi-



(a) Todas as minúcias (verdadeiras e falsas)

(b) Construção da borda erodida



(c) Só as minúcias verdadeiras

Figura 3.32: Processo de eliminação de falsas minúcias. Após a localização das minúcias pelo *crossing number*, determina-se o contorno da ID e elimina-se as minúcias próximas entre si e as próximas do contorno.

nação do ângulo da minúcia. O ângulo das minúcias do tipo terminação é aquele formado pela continuação da crista da ID com o eixo horizontal e do tipo de bifurcação é a aquele formado pela linha que se bifurca. A Figura 2.19 mostra claramente esses ângulos. O método de cálculo do ângulo da minúcia é em parte parecido com o método utilizado na construção do campo direcional.

Neste caso aplica-se uma máscara de 31×31 sobre as posições (x,y) que foram detectadas como minúcias. Na verdade são aplicadas 360 máscaras sobre esta região e cada uma dessas máscaras está associada a um ângulo θ. Por exemplo, a 1ª máscara indica o ângulo zero, portanto multiplica-se elemento a elemento da máscara sobre a região de igual tamanho da imagem da ID centralizada na posição (x,y) (Ver

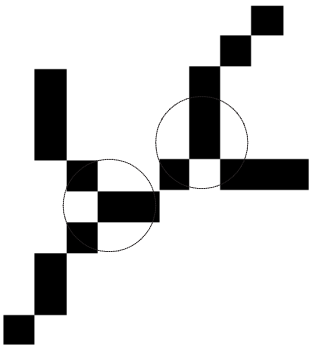


Figura 3.33: Afinamento de uma região de bifurcação com 2 (dois) *pixels* próximos com $cn(p) = 3$.

(a) Imagem Gabor (b) Imagem Negativa

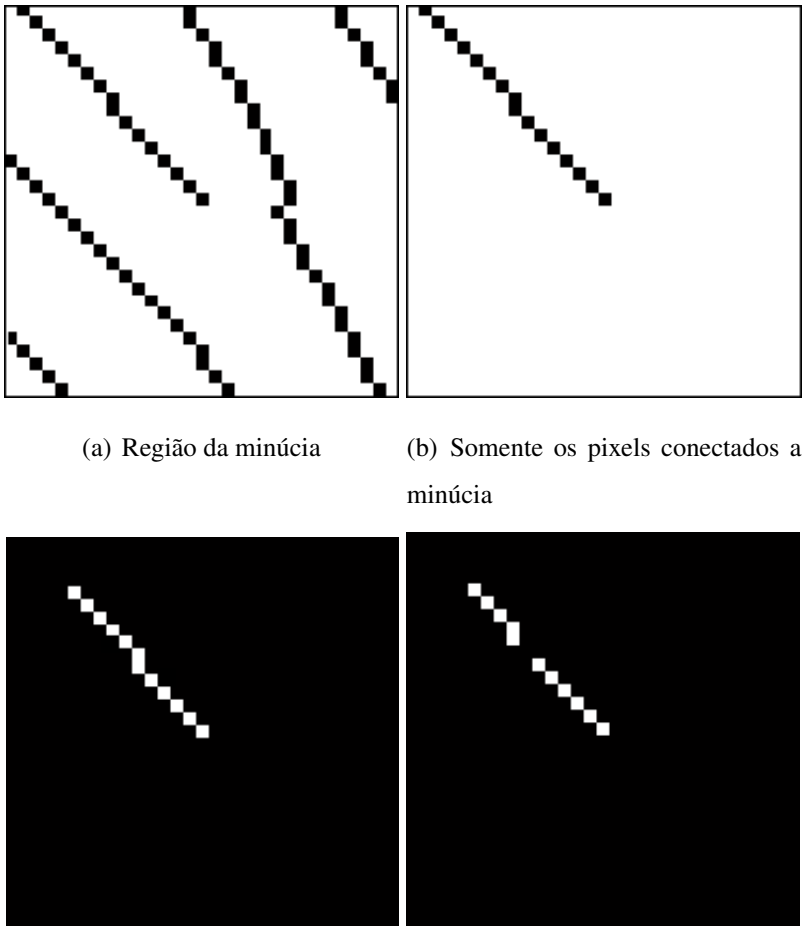
Figura 3.34: Exemplo de uma imagem negativa da ID com o fundo branco.

Equação 3.27). Desta forma, somente os *pixels* da linha ID que são coincidentes com a máscara serão mantidos, por conseguinte a máscara que gerar o maior o número de *pixels* coincidentes indicará o ângulo oposto da minúcia. Isto é, caso a ângulo associado a máscara seja θ tal que $0^o \leq \theta < 180^o$ o ângulo da minúcia será $\theta + 180^o$, caso a ângulo associado a máscara seja θ tal que $180^o \leq \theta < 360^o$ o ângulo da minúcia será $\theta - 180^o$.

$$\theta_{minucia} = max(\sum_{i=1..n} \sum_{j=1..m} M_\theta[i,j].I[i,j]) \tag{3.27}$$

É oportuno ressaltar que uma máscara 31×31 não consegue representar os 360 ângulos, pois há casos que dois ângulos possuem máscaras idênticas. Na verdade, esta máscara consegue representar 344 ângulos diferentes. Antes de aplicar a máscara,

somente os 15 *pixels* conectados mais próximos das minúcias são considerados, logo os *pixels* pertencentes a outras linhas não afetam o cálculo do ângulo. A Figura 3.35 ilustra o processo de determinação do ângulo de uma minúcia.



(a) Região da minúcia (b) Somente os pixels conectados a minúcia

(c) Máscara indicativa do ângulo (d) Pixels coincidentes

Figura 3.35: Processo de determinação do ângulo de uma minúcias. O primeiro passo é selecionar somente os *pixels* conectados ao *pixel* que indica a minúcia, depois aplica-se a máscara indicativa do ângulo da minúcia (multiplicação elemento a elemento), em seguida calcula-se o número de *pixels* coincidentes. O ângulo da minúcia será ângulo oposto da máscara que possuir mais *pixels* coincidentes.

Em suma, o processo de extração de minúcias implementado pode ser descrito pelos passos abaixo:

1. A partir da imagem bruta ID (I_{bruta}) aplica-se a equalização do Histograma;
2. Sobre a imagem da ID equalizada (I_{equali}) no passo 1 aplica-se o filtro de Gabor proposto por Marques (MARQUES, 2004);

3. Sobre a imagem de Gabor (I_{gabor}) gerada no passo 2, inverte-se a luminância de cada pixel gerando a imagem negativa com fundo branco (IN_{gabor});

4. Limiariza-se as imagens I_{gabor} e IN_{gabor} e aplica-se o algoritmo de afinamento às imagens binarizadas, gerando assim as imagens afinadas I_{afina} e IN_{afina};

5. Calcula-se o *crossing number* de todos os *pixels* das imagens I_{afina} e IN_{afina}. Aqueles *pixels* da I_{afina} que retornarem valor igual a 1 (um) são as possíveis posições das minúcias do tipo terminação e os *pixels* da IN_{afina} que também retornarem valor igual a 1 (um) são as possíveis bifurcações. Armazene essas posições em uma matriz M.

6. Para todas as minúcias em M calcula-se a distância entre ela e as demais. Se existir uma distância menor que Δs, ela é excluída de M;

7. Determina-se a borda da imagem e aplica-se o operador de erosão;

8. Exclui-se todas as minúcias de M que estiverem contidas na borda erodida;

9. Para cada *pixel* na posição determinada pelas minúcias em M, determina-se os 15 *pixels* conectados a ele, aplica-se a máscara para determinar o ângulo e armazena-se este valor em M;

Existem outros métodos de detecção de minúcias que não fazem uso de uma imagem afinada. Leung, Engeler & Frank (1990 apud Maltoni et al., 2003), e de maneira similar Marques (MARQUES, 2004), conceberam uma rede neural que classifica as imagens obtidas após o filtro de Gabor em minúcia ou não minúcia. Maio & Maltoni (1997 apud Maltoni et al.,2003) propuseram um método de extração de minúcia que atua diretamente sobre a imagens em tons de cinza. Já outros trabalhos, como de Xiao & Rafar (1991b apud MALTONI et al., 2003) e Kim, Lee & Kim (2001 apud MALTONI et al.,2003), se concentraram mais no pós-processamento que elimina minúcias espúrias.

3.2.3.4 Extração de Outras Características

Por fim, o último descritor a ser extraído da ID é a matriz de características locais (MCL). Basicamente, quase todos os dados contidos nesta matriz são deduzidos do conjunto de minúcias da ID. A razão da construção dessa matriz reside no fato de que os

seus dados são invariantes à rotação e à translação da ID, o que não ocorre como a posição e o ângulo de uma minúcia. A extração da matriz de características locais for proposto Jiang & Yau (2002) e ela é útil no processo de verificação. A única informação da MCL não deduzida do conjunto de minúcias é o número de linhas entre dois pontos que será comentado nos parágrafos seguintes.

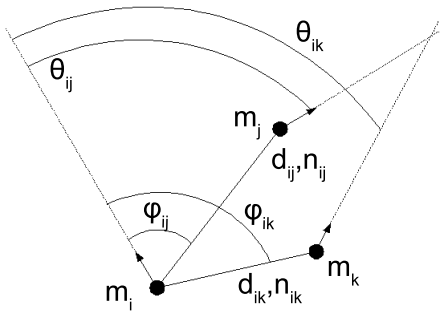


Figura 3.36: As características locais a serem extraídas segundo o método de Jiang & Yau (2002).

A Figura 3.36 apresenta as informações a serem extraídas da ID. Essas características podem ser definidas da seguinte forma: para cada minúcia m_i extraída no processo anterior, identifica-se as duas minúcias (m_j, m_k) mais próximas de m_i; os ângulos θ_{ij} e θ_{ik} são determinados pela diferença angular entre o ângulo da minúcia m_i e os ângulos da minúcia m_j e m_k, respectivamente; os ângulos ϕ_{ij} e ϕ_{ik} são determinados pela diferença angular entre o ângulo da minúcia m_i e os segmentos de reta que ligam a minúcia m_i e as minúcias m_j e m_k, respectivamente; os valores d_{ij} e d_{ik} representam a distância entre a m_i e m_j e entre m_i e m_k, respectivamente; os valores n_{ij} e n_{ik} são definidos como o número de cristas da ID cortadas pelo segmento de reta que une as minúcias m_i e m_j e as minúcias m_i e m_k; t_i, t_j e t_m são os tipos da minúcias de m_i, m_j e m_k. Assim, uma ID digital com n minúcias terá um conjunto de n vetores (v) de características locais, formando uma matriz (MCL) de dimensão igual a $n \times 11$. A Equação 3.28 define os componentes do vetor v.

$$v_i = [d_{ij}, d_{ik}, \theta_{ij}, \theta_{ik}, \phi_{ij}, \phi ik, n_{ij}, nik, t_i, t_j, t_k] \tag{3.28}$$

Não há nenhuma dificuldade em determinar as informações contidas no vetor (v) de características locais, com exceção do número de linhas n_{ij} e n_{ik}. Os valores de θ são facilmente calculados por diferença angular; para calcular os valores de ϕ basta

determinar o ângulo que o segmento correspondente faz com a horizontal e novamente calcular a diferença angular; os valores *d* são as distâncias euclidianas entre as minúcias e os tipos *t* são determinados no processo de extração de minúcias.

Já o processo de cálculo de número de linhas é executado em dois passos: o primeiro passo é determinar o segmento que liga as duas minúcias e o segundo passo é calcular o número de variações de intensidade dos *pixels* presentes neste segmento. O Algoritmo 3.1 descreve a função implementada que determina os *pixels* do segmento de reta que liga duas minúcias. A função *atan*2 usada neste algoritmo calcula o ângulo entre dois pontos retornando um valor entre $]-\pi,\pi]$ e trata as descontinuidades da função tangente.

Algoritmo 3.1 Algoritmo Segmento-de-reta

```
Ponto =
    x:int
    y:int
Segmento = Ponto[]
FUNÇÃO SegmentoReta (p1,p2:  Ponto):Segmento
    seg:Segmento
    ang:  float
    dist:  int
    ang=atan2(p2.y - p1.y,p2.x - p1.x)
    dist=round(sqrt((p2.x - p1.x)^2+(p2.y - p1.y)^2)))
    PARA i de 1 a dist FAÇA
        seg[i].x = cos(ang)*i;
    seg[i].y = sen(ang)*i;
    FIM PARA
    RETORNA seg
FIM FUNÇÃO
```

Para determinar o número de linhas contidas em um segmento de reta basta calcular o número de transições que a intensidade dos *pixels* passa de 1 (branco) para 0 (preto), descontando a primeira transição.

3.2.4 Reconhecimento

Consiste na etapa que determina o grau de similaridade entre a representação da ID a ser reconhecida (Representação da ID de Entrada - ID_{ent}) e a representação da ID já registrada (Representação da ID de Referência - ID_{ref}). É a etapa onde se verifica se duas representações são oriundas da mesma ID ou não. O processo principal do reconhecimento é a verificação que será mostrada na subseção 3.2.4.4. Porém, antes são

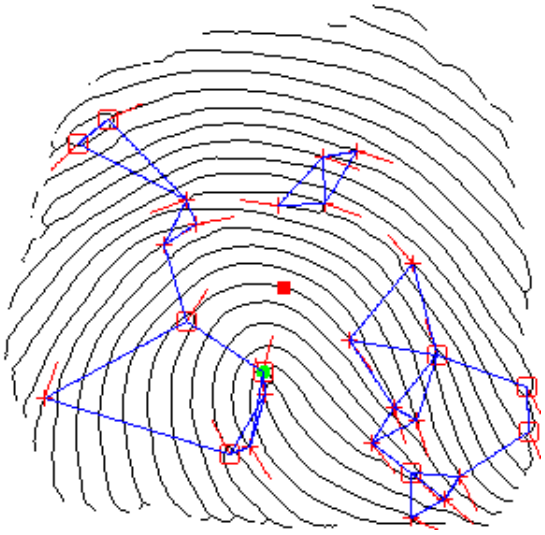


Figura 3.37: Exemplo de uma imagem de ID afinada com segmentos ligando as minúcias.

apresentadas as técnicas de classificação e indexação que são usadas para reduzir o espaço de busca da identificação.

A seguir são enumeradas as principais dificuldades de um processo de reconhecimento (MALTONI et al., 2003).

- **Translação** - Durante o processo de aquisição a ID pode ocupar diferentes lugares no dispositivo, portanto, para cada aquisição, as características ocupam uma posição distinta na imagem resultante;

- **Rotação** - Da mesma forma que a translação, a inclinação da ID no processo de aquisição pode variar, o que leva as características a ocuparem posições diferente;

- **Sobreposição Parcial** - Para cada aquisição a região da ID adquirida pode variar, um par de imagens da mesma ID com pouca região sobreposta acarreta em dificuldade no reconhecimento;

- **Distorção não linear** - O fato de um sensor mapear uma superfície em 3 (três) dimensões através de um contato de 2 (duas) dimensões gera distorções não lineares, o que por conseqüência gera imagens diferentes para a mesma ID;

- **Pressão, Condição da ID e Ruídos** - A pressão no momento da aquisição, a condição da ID e o ruído inerente do processo atuam contra o desempenho do reconhecimento.

3.2.4.1 Classificação

A classificação é o processo que determina a qual classe uma ID pertence. O principal benefício da classificação é promover a redução do espaço de busca no processo de identificação. A identificação é uma comparação $1 : N$, ou seja, a comparação será tão grande quanto o tamanho da base de registros das ID. Sendo assim, convém a redução deste espaço de busca e para isso a classificação é realizada. A maioria dos sistemas de classificação adotam as classes Galton-Henry, as mesmas apresentadas na Seção 2.2.2.1.

Feita a classificação, a identificação não será mais uma comparação $1 : N$, e sim uma comparação $1 : C$ onde C é o número de ID registradas na base de referência que pertencem a mesma classe da ID a ser reconhecida. Infelizmente, as classes não possuem distribuição uniforme (Ver Tabela 2.4) e também há certas ID que não se enquadram perfeitamente em uma única classe.

Mesmo com esses aspectos negativos, a classificação de ID é um estudo que tem atraído um significante número de pesquisa. Estas pesquisas podem ser categorizadas de duas formas: quanto às características utilizadas e quanto a técnicas empregadas. Basicamente, os sistemas classificadores usam 4 tipos de características extraídas da ID: campo direcional, singularidade, desenho das linhas *(ridge line flow)* e as saídas do filtro de Gabor *(Gabor filter responses)* (MALTONI et al., 2003). As técnicas empregadas podem ser categorizadas em 6 grupos: abordagem estatística, abordagem estrutural, abordagem sintática, baseado em rede neurais, baseado em regras e técnicas híbridas (COSTA, 2001), (LIMA, 2002) , (MALTONI et al., 2003), (ERN & SULONG, 2001), (GUO et al., 2003) e (YAGER & AMIN, 2004a). Nos parágrafos seguintes são feitos comentários sobre cada uma dessas abordagens.

A abordagem estrutural se fundamenta na representação de estruturas de alto nível a partir das características ditas como de baixo nível da ID. Por exemplo, algumas regiões semelhantes do campo de direcional da ID se transformam nos vértices de um grafo Ver Figura 3.38). Poderia ser uma árvore, um grafo ou outra estrutura qualquer (BUNKE, 1993 apud MALTONI et al, 2003).

No método proposto por Maio & Maltoni (1996), inicialmente é gerado o campo direcional da ID e depois é feita uma divisão em regiões baseada na similaridade entre os elementos do campo direcional. A etapa seguinte é atribuir a cada região um vértice do grafo e por último o grafo gerado é comparado com um grafo modelo de cada

classe *(graph matching technique)*. A modelo com maior semelhança indicará a classe a que pertence a ID.

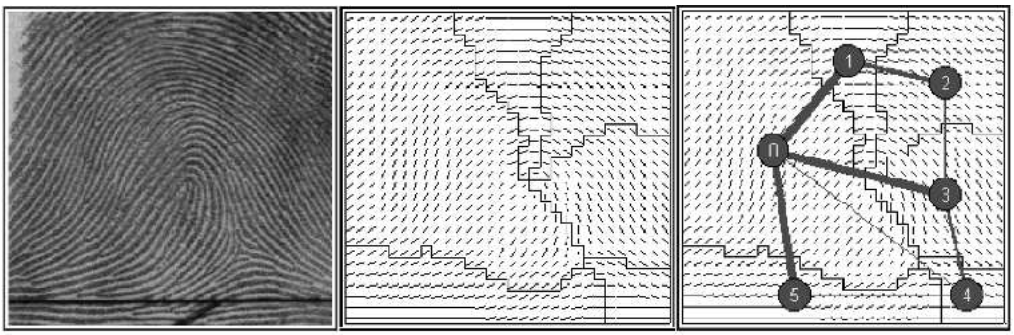
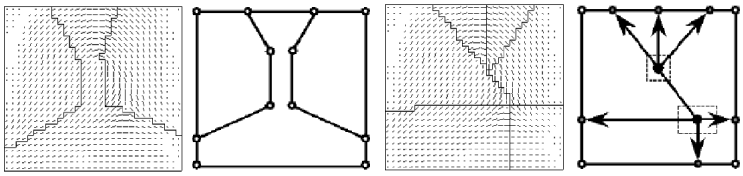


Figura 3.38: Método de classificação proposto por (MAIO & MALTONI, 1996), da esquerda para direita: a imagem bruta, a divisão das regiões e o grafo gerado correspondente.

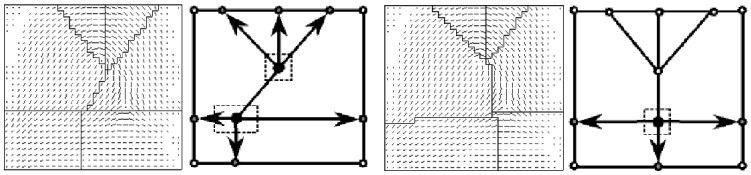
Embora o método descrito no parágrafo anterior seja tolerante em relação a eventuais rotações e translações, não é fácil a tarefa de dividir o campo direcional em regiões homogêneas. Em Capelli & Luminimi (1999), um modelo de classificação baseado em padrões *(teplate-based)* facilita a separação de região distinta de um campo direcional.

Já os classificadores de abordagem sintática descrevem algumas das características da ID por meio de regras ou símbolos, e depois definem uma gramática para cada classe. Desta forma, o processo de classificação é composto por um "parser" que analisa os símbolos extraídos da ID e no fim identifica a classe correspondente. Moayer & Fu (1973, apud MALTONI et al.,2003) construíram um classificador sintático em que os símbolos descritores de uma ID eram associados a pequenos grupos de elementos do campo direcional da ID. Os métodos desta abordagem não logram muito sucesso, principalmente devido a grande diversidade de padrões em uma ID, o que requereria uma gramática complexa (MALTONI et al., 2003)

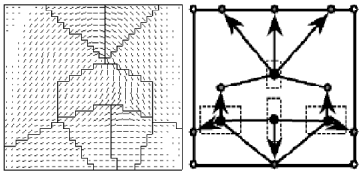
Uma outra abordagem que já produziu muitas publicações é aquela que utiliza redes neurais, os trabalhos de (HALICI & ONGUN, 1996), (MOHAMED & NYONGESA, 2002), (NETO & BORGES, 1997), (DAGHER et al., 2002) e (JIN et al., 2002) são alguns exemplos. A maioria desses trabalhos envolve redes neurais *Multi-Layer Perceptrons* (MLP) que utilizam os ângulos do campo direcional como entrada. Kamijo (1993, apud MALTONI et al., 2003) propõe um arquitetura composta por várias redes MLP, cada uma treinada para reconhecer ID pertencente a uma classe diferente. Bowen (1992, apud MALTONI et al.,2003) propôs duas redes neurais disjuntas, uma recebe a posição de um



(a) Classe Arco Plano*(Arch)* (b) Classe Presilha Direita *(Left Loop)*



(c) Classe Presilha Esquerda *(Right Loop)* (d) Classe Arco Angular *(Tented Arch)*



(e) Classe Verticilo *(Whorl)*

Figura 3.39: As regiões da ID e o esquema gerado para cada uma da 5 classes (CAPPELLI & LUMINI, 1999).

ponto singular e a outra os elementos do campo direcional, as saídas dessas redes são passadas para outra rede que produz a classificação final.

Na abordagem por regras é similar ao trabalho de um perito. Na hora de classificar uma ID um papiloscopista analisa o tipo e a posição das singularidades presentes na ID. Por exemplo, uma ID sem nenhuma singularidade seria classificada como da classe Arco. Os sistemas baseados em regras utilizam o mesmo conceito, sendo nada mais que uma automatização da classificação feita por papiloscopistas. É uma abordagem simples e que funciona quando as singularidades são de fácil detecção. Entretanto, quando o modo de aquisição da ID for do tipo batida a classificação terá seu desempenho comprometido, pois dificilmente a imagem capturada conterá todas as singularidades da ID.

Em Kawagoe & Tojo (1984 apud MALTONI et al, 2003), é apresentado um método que extrai as singularidades pelo índice de Poincaré (Seção 3.2.3.2), depois faz uma classificação preliminar de acordo com a Tabela 3.3 e por fim executa uma classificação refinada. Esta última faz uso da inclinação central para distinguir as classes da

Tabela 3.3: Técnica de classificação proposta por Kawagoe & Tojo (1984 apud MALTONI et al, 2003).

Classe da ID	**Singularidades**
Arco Plano *(Arch)*	Nenhuma Singularidade
Arco Angular, Presilha Esquerda e Presilha Direita *(Tented Arch, Right Loop e Left Loop)*	Um Núcleo e Um Delta
Verticulo *(Tented Arch)* *(Whorl)*	Dois Núcleos e Dois Deltas

segunda linha da Tabela 3.3.

Em Karu & Jain (1984 apud MALTONI et al., 2003) um método com uma regulagem iterativa é usado para validar as singularidades extraídas a partir do campo direcional. Deste modo, não há detecção de falsa singularidade o que aumenta a acurácia da classificação. Neste trabalho também é proposto um método para distinguir os arcos *(tented arch)* dos núcleos *(loops)*, para isso é calculado a média da distância entre uma linha que liga duas singularidades e as direções do campo direcional. Trabalhos com abordagens parecidas podem ser encontrados em Ratha et al. (1996 apud MALTONI et al., 2003); Ballan, Sakarya & Evans (1997 apud MALTONI et al, 2003) e Bartesaghi, Sakarya & Evans (1997 apud MALTONI et al., 2003). Por fim, o trabalho de Hong & Jain (1999) propõe um método mais robusto. O algoritmo concebido utiliza tanto com as singularidades quanto com os desenhos das linhas da ID.

Por fim, a Tabela 3.4 apresenta diversas publicações científicas a respeito de classificação de ID. Esta tabela mostra as características utilizadas e a técnica do classificador.

3.2.4.2 Indexação

Assim como a classificação, a indexação possui o objetivo de reduzir o espaço de busca para o processo de identificação. No entanto, ela não atua na divisão da ID em classes, e sim indexa as ID a partir de outras características. A indexação se torna útil, pois mesmo após a classificação não há uma redução satisfatória do espaço de busca. Portanto, cabe a esta etapa separar as ID em mais categorias que por sua vez teriam um menor número de ID.

A primeira tentativa em subclassificar as ID veio dos especialistas de identifi-

Tabela 3.4: Histórico das técnicas de classificação. A coluna características indica quais descritores o trabalho utilizou (O - Campo Direcional, S - Singularidades, L - Linhas da ID e G - Gabor). A coluna classificador indica a abordagem usada na classificação (R - Baseado em Regras, S - Sintático, E - Estrutural, RN - Redes Neurais e H - Híbrido). (MALTONI et al., 2003)

	Características				**Classificador**					
Métodos de Classificação	**O**	**S**	**L**	**G**	**R**	**S**	**E**	**Es**	**RN**	**H**
Moayer & Fu (1975)	√						√			
Moayer & Fu (1976)	√						√			
Rao & Balck (1980)	√						√			
Kawagoe & Tojo (1984)		√	√			√				
Hughes & Green (1991)	√								√	
Bowen (1992)	√	√							√	
Kamijo, Mieno & Kojima (1992)	√								√	
Moscinska & Tyma (1993)	√				√				√	
Kamijo (1993)	√								√	
Wilson, Candela & Watson (1994)	√								√	
Omidvar, Blue & Wilson (1995)	√								√	
Candela et al (1995)	√		√		√				√	√
Maio and Maltoni (1996)	√						√			
Halici & Ongun (1996)	√								√	
Karu & Jain (1996)		√			√					
Chong et al (1997)			√		√					
Ballan, Sakarya & Evans (1997)		√			√					
Chong et al (1997)		√			√					
Senior (1997)			√		√					
Wei, Yuan & Jie (1998)	√			√					√	√
Cappelli et al (1999)	√						√			
Lumini, Maio & Maltoni (1999)	√						√			
Jain, Prabhakar & Hong(1999)				√			√			
Hong & Jain (1999)				√			√			
Cappelli, Maio & Maltoni (1999)				√			√			

cação civil. Em 1984 o FBI possuía um procedimento que categorizava as ID de acordo com os números de linhas entre singularidades (FBI, 1984 apud MALTONI et al, 2003). Era um procedimento realizado por especialistas e a subclassificação também dependia de outras informações, como por exemplo, se a digital era do polegar, dedo médio ou dedo indicador. Por sua alta complexidade, poucas pesquisas tentaram implementá-lo.

3.2.4.3 Identificação

O processo de identificação nada mais é que a repetição de *n* processos de verificação, onde *n* é o números de ID previamente registradas. Ou seja, é o reconhecimento que não possui o conhecimento prévio do indivíduo a ser identificado, é a comparação

(matching) $1:N$. A identificação pode ser realizada de três formas (TAN et al., 2003b):

1. **Identificação propriamente dita**

   É a identificação baseada somente na verificação, ou seja, é executada a verificação da ID de entrada com todas ID de referência registradas. Portanto, é uma forma muito dispendiosa, consumindo muito tempo na busca da ID de referência como maior similaridade. Tornando-se assim, praticamente inviável para aplicações reais.

2. **Identificação com classificação**

   Nesta forma, a etapa de classificação é executada anteriormente. A busca é executada somente sobre as ID da mesma classe que a ID de entrada. Mesmo assim, não há uma redução expressiva do espaço de busca, pois há classes que correspondem a aproximadamente 30% da população de ID.

3. **Identificação com indexação**

   De forma parecida a anterior, exceto pelo fato da busca ocorrer sobre as ID indexadas de maneira similar a ID de entrada.

3.2.4.4 Verificação

A verificação é o núcleo do processo de reconhecimento *(matching)*. É a subetapa que realiza de fato a comparação entre a ID de Entrada com a ID de Referência. Há uma enorme produção de trabalhos científicos que tratam do assunto verificação de ID, entre eles pode-se destacar (DAGHER et al., 2002), (GAO & MOSCYTZ, 2004), (GERMAIN et al., 1997), (HAO et al., 2002), (JAIN & HONG, 1996), (JIA et al., 2004), (JIANG & YAU, 2002), (JIN et al., 2002), (KOVACS-VAJNA, 2000), (LE et al., 2001), (LEE & NAM, 1999), (LEE & WANG, 1999), (MOHAMED & NYONGESA, 2002), (PRABHAKAR, 2001), (SALEH & ADHAMI, 2001), (SHA & TANG, 2004), (SHAH & SASTRY, 2004), (TAN & BHANU, 2002), (TICO & KUOSMANEN, 2003) e (YAGER & AMIN, 2004b). Entretanto, mesmo havendo várias abordagens os métodos de verificação podem ser categorizados em três principais grupos: os métodos baseados na correlação *(correlation-based matching)*, os métodos baseados nas minúcias *(minutiae-based matching)* e os métodos baseados nas características gerais *(ridge feature-based*

matching).

- Métodos Baseados na Correlação

Determina a correlação entre duas imagens de uma ID, quanto maior a correlação maior será o grau de similaridade entre as duas imagens. Seja $R(x,y)$ a imagem de uma ID de referência e $E(x,y)$ a imagem de uma ID a ser verificada, a correlação entre as imagens é dada pela Equação 3.29 no domínio do espaço e pela Equação 3.30 no domínio da freqüência (CHIKKERUR, 2005). Neste método, o processo de verificação consiste em buscar o ponto de valor máximo *(peak magnitude)* na imagem da correlação. A posição do ponto máximo indica a translação entre as imagens R e E e o valor deste ponto determina o grau de similaridade (Ver Figura 3.40 e 3.41).

$$I_c(k,l) = \sum_x \sum_y R(x+k, y+l)E(x,y) \tag{3.29}$$

$$I_c(k,l) = FFT^{-1}\{FFT(R)FFT^*(E)\} \tag{3.30}$$

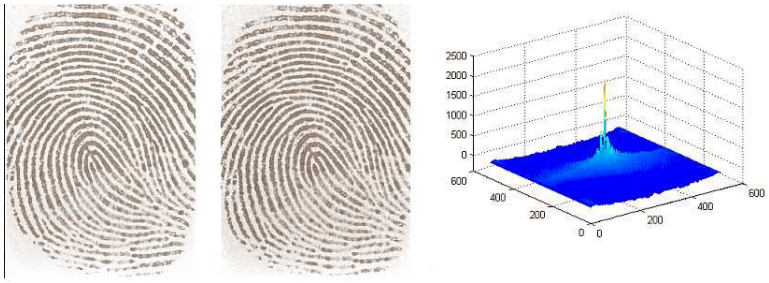


Figura 3.40: Correlação entre duas imagens da mesma ID. Nota-se que na imagem da xorrelação existe um ponto de valor alto (CHIKKERUR, 2005).

Este processo não requer imagens de alta resolução e é rápido desde que a correlação seja implementada através de técnicas óticas (CHOUDHARY & AWWAL, 1999; LEE et al., 1999; ROBERGE et al., 1999 apud CHIKKERUR, 2005). Entretanto, como a correlação envolve as característica globais da imagem, é necessário cuidado no processo de aquisição da ID pois a correlação não é invariante a translação nem a rotação. Além disso, os métodos baseados na correlação têm seu desempenho afetado quando há

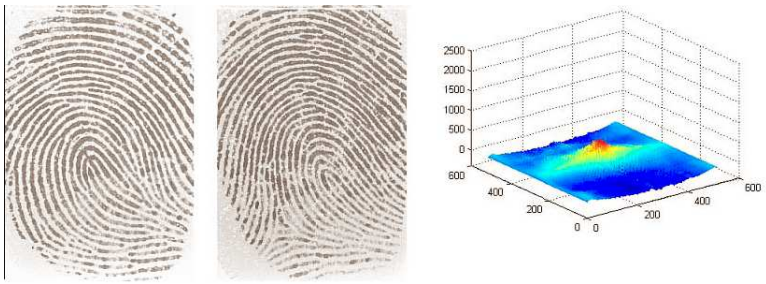


Figura 3.41: Correlação entre duas imagens ID distintas. Nota-se que na imagem da correlação não há ponto de valor alto (CHIKKERUR, 2005).

distorção não linear entre as imagens.

- Baseado nas Características Gerais

Esta é uma abordagem recente que veio com intuito de aumentar a robustez do processo de verificação. Acrescentando o número de descritores com o propósito de não ficar dependente da extração das minúcias. Entre esses descritores acrescidos, destacam-se os seguintes (MALTONI et al., 2003)

- tamanho e forma da silhueta da ID;
- número, tipo e posição das singularidades;
- relação espacial e atributos geométricos das linhas da ID (XIAO & BIAN, 1986 apud MALTONI et al., 2003) e (KAYNAZ & MITRA, 1992 apud MALTONI et al., 2003);
- informações sobre a textura da ID;
- poros (STOSZ & ALYEA, 1994 apud MALTONI et al., 2003);
- características fractais (POLIKARPOVA, 1996 apud MALTONI et al., 2003);

- Métodos Baseados nas Minúcias

A verificação de ID baseada nas minúcias é sem dúvida a técnica mais difundida e usada, fato justificado por ser o mesmo método utilizado pelos papiloscopistas e por ser aceito em instituições jurídicas (MALTONI et al., 2003).

Este método pode ser definido da forma a seguir: seja ID_{ref} a impressão digital de referência e ID_{ent} a impressão digital de entrada, após o processo de extração de minúcias ambas ID são representadas pelos seus respectivos conjuntos de minúcias M_{ref} e M_{ent} (Equações 3.31 e 3.32). O problema consiste em determinar se os conjuntos M_{ref} e M_{ent} representam a mesma ID ou não.

$$M_{ref} = \{m_1, m_2, \ldots, m_m\}, \quad m_i = \{T_i, x_i, y_i, \theta_i\}, \quad i = 1 \ldots m \tag{3.31}$$

$$M_{ent} = \{m_1, m_2, \ldots, m_n\}, \quad m_j = \{T_j, x_j, y_j, \theta_j\}, \quad j = 1 \ldots n \tag{3.32}$$

As principais dificuldades deste método são:

- Os conjuntos não são ordenados e podem ter cardinalidade distintas;
- Devido a posição da ID e o modo de contato no momento da aquisição, os conjuntos de minúcias podem diferir quanto a rotação, translação, escala e outras distorções não lineares;
- Uma minúcia m_i em M_{ref} pode não ter uma minúcia m_j correspondente em M_{ent};
- Por outro lado m_j em M_{ent} pode não estar associada a nenhuma outra minúcia em M_{ref};

Este tipo de problema aparece em diversas áreas de conhecimento e é classificado como um problema de *point pattern matching*. O trabalho de Li et al. (LI et al., 2003) faz uma revisão sobre todas as técnicas empregadas para solucionar o problema de *point pattern matching*. Esta revisão separa as técnicas em dois grupos principais: transformação rígida e *affine (ridge/affine motion)* e transformação não rígida ou elástica *(non ridge/elastic motion)*.

Li et al. (2003) enumera as seguintes técnicas como pertencentes ao primeiro grupo: categorização *(clustering)*, *relaxation*, *inter-point distances*, comparação de cadeias de caracteres *(string matching)*, busca em grafos *(Graphs with tree searching)* etc. E ao segundo grupo: *piecewise approximation* , *elastic/deformable models* e *weighted-graph matching*.

A metodologia escolhida e implementada neste trabalho para resolver o problema do *point pattern matching*, foi a transformação rígida baseado nas diferenças entre

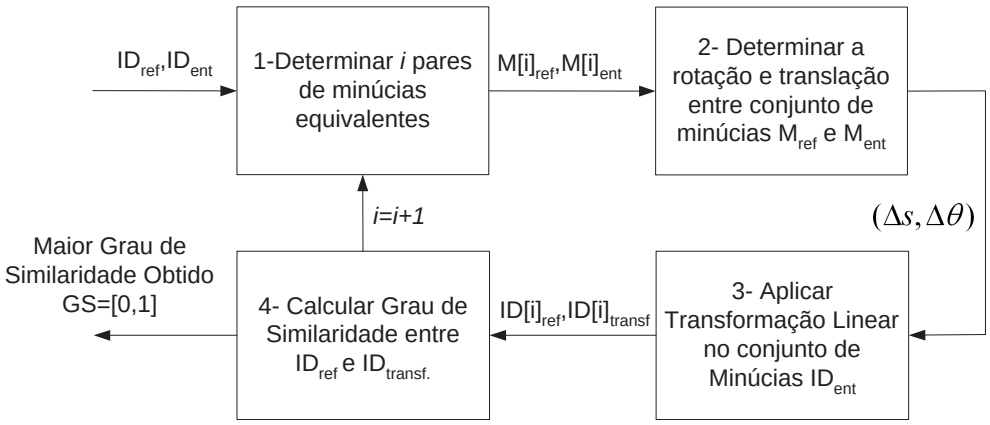


Figura 3.42: Etapas do processo de verificação baseado na transformação linear do conjunto de minúcias.

as minúcias equivalentes. Sendo assim, é aplicado uma transformação linear sobre o conjunto M_{ent} e em seguida é medido o grau de similaridade entre o conjunto M_{ref} e conjunto M_{ent} transformado.

Os passos do método de verificação estão ilustrados no esquema da Figura 3.42. O primeiro passo é determinar um subconjunto de minúcias equivalentes entre os conjuntos M_{ref} e M_{ent}. Escolhido este subconjunto, determina-se a translação (δs) e rotação $(\delta\theta)$ entre as minúcias de M_{ref} e M_{ent}. De posse dos valores de δs e $\delta\theta$ aplica-se a transformação linear sobre M_{ent}. Obtendo-se M_{ent} o conjunto M_{transf}. A última etapa é o cálculo do grau de similaridade entre M_{ref} e M_{transf}. Nota-se que para cada par de minúcias obtidas no primeiro passo (Ver Figura 3.42), aplica-se os 3 passos seguintes. O grau de similaridade final será o maior grau de similaridade obtido nesta iteração. A seguir, esses 4 (quatro) passos são discutidos.

Foram concebidos 4 (quatro) métodos de determinação de minúcia equivalente: centróide, exaustivo, singularidade e características locais.

O método do centróide seleciona as três minúcias de M_{ref} mais próximas do centro da imagem da ID_{ref} e as três minúcias M_{ent} mais próximas do centro da imagem de ID_{ent}. Portanto, é repassado para os passos seguintes as combinações entre essas minúcias. Desta forma, este método gera 6 iterações dos passos 2, 3 e 4. O resultado final deste processo de verificação será o maior grau de similaridade obtido nestas 6 iterações.

O método da singularidade funciona de maneira similar, exceto pelo fato deste selecionar as três minúcias de M_{ref} e de M_{ent} mais próxima de uma singularidade. Para

as ID com mais de uma singularidade, aquela que for mais próxima do centróide será a selecionada e caso não exista singularidade o ponto de referência será o centróide. Neste método também haverá 6 iterações dos passos 2, 3 e 4 e o resultado final será o maior grau de similaridade obtido nestas 6 iterações.

Já o método exaustivo utilizada todas as minúcias de M_{ref} e M_{ent}, portanto haverá neste método n pares de valores de δs e $\delta\theta$ onde $n = |M_{ref}|.|M_{ent}|$. De maneira análoga aos métodos anteriores, neste método haverá n iterações dos passos 2, 3 e 4. O resultado final será o maior grau de similaridade obtido nestas n iterações.

O último método de determinação de minúcias equivalentes é o de características locais. Em vez de selecionar as minúcias baseado na região que ela ocupa, este método analisa a matriz de características locais (MCL) gerada para cada conjunto M_{ref} e M_{ent}. A linha i da MCL_{ref} indica as características locais da minúcia m_i, ou seja, o vetor v_i da MCL_{ref} carrega informações relativas as distâncias, as diferenças angulares e o números de linhas entre a minúcia m_i e suas minúcias vizinhas mais próximas. Sendo assim, caso o conjunto M_{ent} represente a mesma ID que M_{ref}, há um grande probabilidade de existir um vetor v_j da MCL_{ref} similar a um vetor v_i da MCL_{ent}. Esta probabilidade varia de acordo com o desempenho do processo de extração de minúcias, isto é, se não houver nenhuma minúcia ausente ou minúcia espúria maior será a similaridade entre os vetores v_i e v_j.

Desta forma, a escolha das minúcias equivalentes será baseada no grau de similaridade entre os vetores da MCL_{ref} e da MCL_{ent}. Serão selecionados 3 (três) pares de minúcias com maior similaridades entre os seus respectivos vetores da *MCL*. Para esses 3 (três) pares de minúcias equivalentes geram-se 3 (três) pares de valores de δs e $\delta\theta$, e de maneira análoga aos métodos anteriores, haverá 3 iterações dos passos 2, 3 e 4. O resultado final será o maior grau de similaridade obtido nestas 3 iterações.

O grau de similaridade entre os vetores da MCL_{ref} e da MCL_{ent} é determinado pela distância euclidiana dos mesmos, conforme exposto na Equação 3.33. Como as componentes dos vetores representam grandezas diferentes, o vetor do *MCL* foi normalizado pelo $z - score$. Isto é, em um conjunto com n matrizes de características locais foi calculada a média e o desvio padrão de cada coluna da *MCL*. Os valores da *MCL* foram normalizados de acordo como a Equação 3.34.

$$D(v_i, v_j) = \sqrt{\sum_{k=1}^{11} (v_i(k) - v_j(k))^2} \tag{3.33}$$

$$v_i(k) = \frac{v_i(k) - \mu v_i(k)}{\sigma v_i(k)} \tag{3.34}$$

Terminada a escolha dos pares de minúcias equivalentes, é determinada a translação (δs) e a rotação ($\delta\theta$) entre as minúcias M_{ref} e M_{ent}. Os valores δs e $\delta\theta$ são obtidos pela diferença entre a minúcia (m_{ref}) equivalente de M_{ref} e a a minúcia (m_{ent}) equivalente de M_{ent}, conforme as Equações 3.35 e 3.36.

$$\delta s(x,y) = m_i(x,y) - m_j(x,y) \tag{3.35}$$

$$\delta\theta = m_i(\theta) - m_j(\theta) \tag{3.36}$$

Determinado os valores de δs e $\delta\theta$, inicia-se a transformação linear conforme a Equação 3.37.

$$\begin{bmatrix} x'_j \\ y'_j \end{bmatrix} = \begin{bmatrix} cos\ \delta\theta & -sen\ \delta\theta \\ sen\ \delta\theta & cos\ \delta\theta \end{bmatrix} \begin{bmatrix} x_j \\ y_j \end{bmatrix} + \begin{bmatrix} \delta x \\ \delta y \end{bmatrix} \tag{3.37}$$

Os passos 1, 2 e 3 do esquema da Figura 3.42 estão descritos a seguir:

1. Seja M_{ref} o conjuntos de minúcias da ID de referência e M_{ent} o conjunto de minúcias da ID de entrada. A partir de um método implementado (centróide, exaustivo, singularidade e características locais), identificam-se os pares de minúcias equivalente (m_i, m_j). Para todos esses pares executam-se os passos seguintes.

2. Calcula-se a diferença espacial $(\delta s(x,y))$ e angular $(\delta\theta)$ entre m_i e m_j, dadas pelas Equações 3.38 e 3.39, respectivamente;

$$\delta s(x,y) = m_i(x,y) - m_j(x,y) \tag{3.38}$$

$$\delta\theta = m_i(\theta) - m_j(\theta) \tag{3.39}$$

3. Para todos os elementos de $M_{ent}(x,y)$ soma-se o valor de δs conforme a Equação 3.40;

$$\forall M_{ent}(x,y) \quad \text{faça} \quad m(x,y) = m(x,y) + \delta S(x,y) \tag{3.40}$$

4. Armazena-se os valores m_j em m_{jtmp};

5. Para todos os elementos de $M_{ent}(x,y)$ subtrai-se o valor de $m_j(x,y)$ conforme a Equação 3.44;

$$\forall M_{ent}(x,y) \quad \text{faça} \quad m(x,y) = m(x,y) - m_i(x,y) \tag{3.41}$$

6. Rotaciona-se em $\delta\theta$ todos os elementos de $M_{ent}(x,y)$ de acordo com a Equações 3.42 e 3.43

$$\forall M_{ent}(x) \quad \text{faça} \quad m(x) = cos(\delta\theta).x - sen(\delta\theta).y \tag{3.42}$$

$$\forall M_{ent}(y) \quad \text{faça} \quad m(y) = sen(\delta\theta).x + cos(\delta\theta).y \tag{3.43}$$

7. Para todos os elementos de $M_{ent}(\theta)$ soma-se o valor de $\delta\theta$ conforme a Equação 3.44;

$$\forall M_{ent}(\theta) \quad \text{faça} \quad m(\theta) = m(\theta) + \delta\theta \tag{3.44}$$

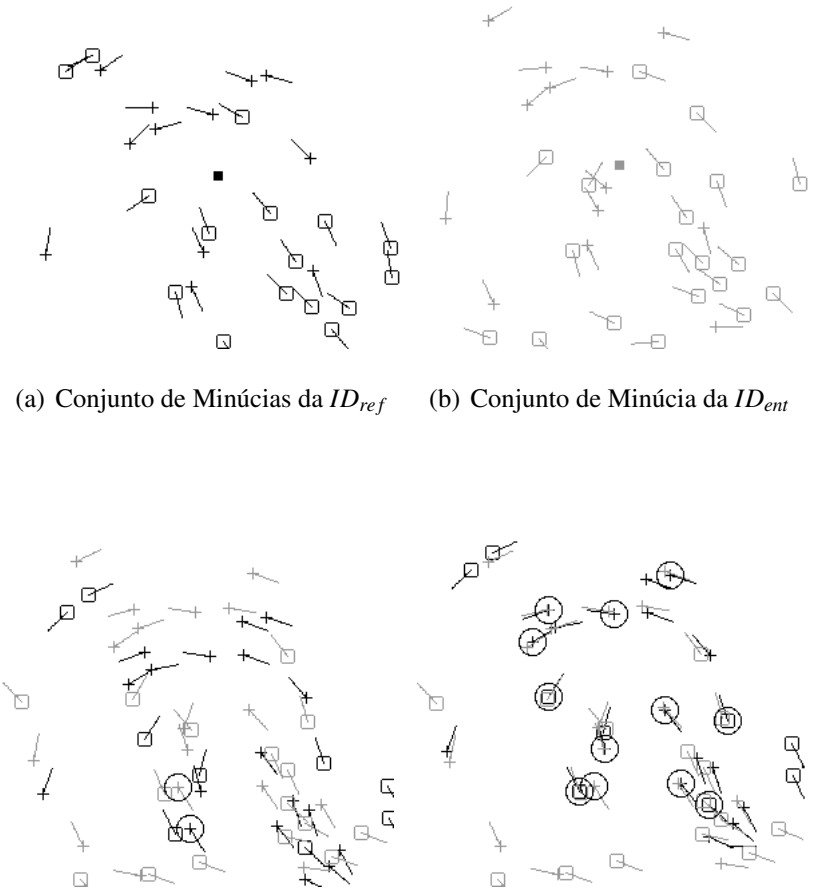
8. Para todos os elementos de $M_{ent}(\theta) \geq 360^{o}$ faz-se $M_{ent}(\theta) = 360^{o} - M_{ent}(\theta)$

9. Para todos os elementos de $M_{ent}(x,y)$ soma-se o valor de $m_{jtmp}(x,y)$ conforme a Equação 3.45;

$$\forall M_{ent}(x,y) \quad \text{faça} \quad m(x,y) = m(x,y) + m_{jtmp}(x,y) \tag{3.45}$$

A Figura 3.43 ilustra um exemplo de transformação linear sobre o conjunto de minúcias da ID_{ent}. Nota-se que nas Figuras 3.43(a) e 3.43(b) as respectivas minúcias equivalentes estão envolvidas por um círculo. A Figura 3.43(c) mostra as sobreposição

dos dois conjuntos de minúcias sem a transformação linear sobre as minúcias de ID_{ent}. Já a Figura 3.43(d) apresenta a sobreposição com transformação linear e as minúcias correspondentes são envolvidas por um círculo.



(a) Conjunto de Minúcias da ID_{ref} (b) Conjunto de Minúcia da ID_{ent}

(c) Sobreposição dos Dois Conjuntos (d) Sobreposição dos Dois Conjuntos após a Transformação Linear

Figura 3.43: Ilustração da transformação linear do conjunto de minúcias da ID_{ent} e a indicação das minúcias correspondentes (círculo em volta) para $\Delta s = 10$ e $\Delta\theta = 10$.

O conjunto resultante M_{ent} é então chamado de conjunto M_{transf}, e daí é determinado o grau de similaridade. Uma minúcia m_i será considerada correspondente a m'_j, gerada após a transfomação, se atender as Equações 3.46 e 3.47.

$$\delta s(m'_j, m_i) = \sqrt{(x_i - x'_j)^2 + (y_i - y'_j)^2} \leq \Delta s \tag{3.46}$$

$$\delta\theta(m'_j, m_i) = min(|\theta_i - \theta'_j|, 360 - |\theta_i - \theta'_j|) \leq \Delta\theta \tag{3.47}$$

O grau de similaridade entre os conjuntos M_{ref} e M_{transf} é determinado conforme os passos abaixo:

1. Seja ΔS, $\Delta\theta$ e n os parâmetros do processo de verificação. Os dois primeiros parâmetros determinam se um par de minúcias será considerado similar, e o terceiro parâmetro indica número mínimo de minúcias similares para haver verificação positiva. Seja *Acumulador* a variável que totaliza o número de minúcias similares;.

2. Inicia-se *Acumulador* igual a -1;

3. Para cada minúcia m_i do conjunto M_{ref}, calcula-se a distância euclidiana (Equação 3.46) entre a minúcia m_i e todas as minúcias do M_{transf}. Seleciona-se a minúcia de M_{transf} mais próxima de m_i e calcula-se a diferença angular entre elas (Equação 3.46);

$$\delta s(m_i, m'_j) = \sqrt{(m_i(x) - m'_j(x))^2 + (m_i(y) - m'_j(y))^2} \tag{3.48}$$

$$\delta\theta(m_i, m'_j) = min(|m_i(\theta) - m'_j(\theta)|, 360^{\circ} - |m_i(\theta) - m'_j(\theta)|) \tag{3.49}$$

4. Caso $\delta s > \frac{\Delta s}{2}$ ou $\delta > \frac{\Delta\theta}{2}$ atribui-se a Grau de Similaridade de Minúcias (GVM) valor 0 (zero) e vá para o passo 6;

5. Caso $\delta s \leq \frac{\Delta s}{2}$ e $\delta\theta \leq \frac{\Delta\theta}{2}$ atribui-se a Grau de Similaridade de Minúcias (GVM) valor 1 (um), caso contrário atribua a Grau de Similaridade de Minúcias (GVM) o valor da Equação 3.50;

$$2.\left(\frac{\Delta s - \delta s}{\Delta s}.\frac{\Delta\theta - \delta\theta}{\Delta\theta}\right) \tag{3.50}$$

6. Adiciona-se ao valor do *Acumulador* o valor de GVM;

7. Repeti-se os passos 3 a 7 até percorrer todos elementos de M_{ref};

8. Calcula-se o valor do Grau de Similaridade da Verificação de acordo com a Equação 3.51

$$GSV = \frac{Acumulador}{n} \tag{3.51}$$

9. Aplica-se em GSV a função definida na Equação 3.52.

$$GSV \begin{cases} 1 & \text{se } GSV > 1 \\ GSV & \text{caso contrário} \end{cases} \tag{3.52}$$

Finalizado o processo de verificação, a etapa de Reconhecimento repassa o grau de similaridade calculado para etapa de Decisão e caberá a esta etapa anunciar se o reconhecimento foi positivo ou negativo.

3.2.5 Decisão

Como se pode aferir na Figura 2.3, a etapa de Decisão é a última de um Sistema Biométrico. É nesta etapa que se define os parâmetros do sistema, como por exemplo, qual será o limiar que determina um reconhecimento positivo ou negativo. Basicamente, certas definições sobre o Sistema Biométrico estão relacionadas como o ambiente e o propósito do sistema em questão. Informações como aquelas mencionados na Seção 2.1.2.1 devem ser consideradas pela Etapa de Decisão, bem como medidas que variam os limiares da SB em situação de tentativa de fraude.

3.3 Protótipo Concebido

O propósito desta pesquisa é investigar o processo de reconhecimento de identidade, e como parte desta investigação foi implementado algumas técnicas empregadas deste processo. Então, fez-se necessário a construção de um protótipo que tanto agregasse esta implementação quanto auxiliasse a avaliação destas técnicas. Ao protótipo concebido deu-se o nome de IDSDK, ele foi construído através da ferramenta científica MATLAB e a Figura 3.44 ilustra sua tela principal.

Através do IDSDK foi possível aferir todos os passos dos processos implementados, desta forma qualquer funcionamento inesperado era conhecido, e também foi possível avaliar os resultados de maneira eficiente. Este protótipo fica como uma das contribuições desta pesquisa. Entre as funcionalidades do IDSDK, destacam-se as seguintes:

- Operações de processamento de imagem, como por exemplo, afinamento, limiarização, erosão, dilatação, abertura, fechamento, detecção de borda, preenchimento etc;

Figura 3.44: Protótipo desenvolvido - IDSDK

- Visualização dos processos implementados e etc.
- Extração de características da ID:
  - Construção do campo direcional - com as opções de número de direções, tamanho da máscara e método de suavização;
  - Extração de singularidades pelo método de índice de Poincaré;
  - Extração de singularidades pelo método proposto por Jain et. al (JAIN et al., 2000);
  - Extração de minúcias através do cálculo do *crossing number* sobre a imagem afinada;
  - Extração da matriz de características locais;
- Verificação de Impressões Digitais:
  - Método do Centróide;
  - Método Exaustivo;
  - Método das Singularidades

– Método por Características Locais;

Conforme mostrado na Figura 3.44, o protótipo desenvolvido permite a comparação visual entre duas imagens da ID. Desta forma, foi possível aferir e comparar os processos implementados. Pelo protótipo também é possível a navegar sobre a imagem carregada, isto é, pode-se ampliar a imagem, verificar a posição e a luminância de um *pixel* qualquer da imagem, verificar os atributos de uma minúcia pela imagem, salvar as imagens resultantes etc. Outra facilidade implementado foi o processamento por lote que permite aplicar uma operação sobre várias imagens de ID. Por fim, pelo IDSDK é possível visualizar o resultado do método de verificação mostrando o conjunto de minúcias transformado e as minúcias equivalentes.

3.4 Considerações Finais

Era o objetivo deste capítulo expor as principais técnicas de cada etapa de um processo de reconhecimento de identidade por impressão digital. De maneira nenhuma este texto produzido esgota o assunto, no entanto ele mostra as principais estratégias para resolver os problemas intrínsecos de cada processo. No próximo capítulo é apresentado os resultados obtidos para as técnicas implementadas.

4 TESTES E MÉTRICAS DE DESEMPENHO

"Espere o melhor, prepare-se para o pior e receba o que vier."

Provérbio Chinês

4.1 Considerações Iniciais

Nas últimas décadas, as atividades relativas aos Sistemas Biométricos baseados em impressões digitais cresceram significativamente. Este crescimento provocou o surgimento de vários grupos de pesquisa tanto no âmbito acadêmico quanto industrial. Por conseqüência, houve um expressivo aumento na produção de novos dispositivos e novas técnicas a serem utilizadas nos SB. Contudo, não houve um devido cuidado na hora de se padronizar as formas de testes e as métricas de avaliação. Ou seja, cada trabalho produzido tinha a sua base particular de imagens de teste e seu critério particular de avaliação. Tornando assim inviável qualquer forma de comparação entre as pesquisas desenvolvidas.

Inicialmente, para contornar o problema de haver bases de imagens de testes diferentes, os desenvolvedores passaram a utilizar as imagens de ID de domínio público disponibilizadas pelo Instituto Americano de Padrões e Tecnologia (NIST). Entretanto, essas imagens diferem das imagens normalmente empregadas em um PRIID. As imagens do NIST são *scaneadas* de registros públicos de identificação, geralmente são do tipo rolada e possuem muitos ruídos. Portanto, não representam fielmente os tipos de imagens que são adquiridas por um PRIID.

Sendo assim, para suprir a ausência de padrões de base de teste ou de forma de avaliação foi instituída uma Competição de Sistemas de Verificação de Impressões Digitais (FVC). Proporcionando assim uma comparação factível tanto entre os métodos publicados na literatura científica quanto entre os produtos comerciais do mercado. Esta iniciativa foi o primeiro passo na busca de uma padronização, pois nesta competição os

algoritmos são submetidos às mesmas bases de imagens de ID e são avaliados seguindo o mesmo critério de avaliação (MAIO et al., 2002a), (MAIO et al., 2002b) e (MAIO et al., 2004). A FVC ocorre de dois em dois anos e o número de instituições acadêmicas e empresas comerciais que participam aumenta a cada competição.

4.2 Base de Testes

Neste trabalho fez-se uso de 12 bases distintas num total de 10.560 imagens, que foram aplicadas nos FVC dos anos de 2000, 2002 e 2004. As imagens do FVC/2000 e FVC/2002 estão disponíveis na obra de Maltoni et al (2003) e as imagens do FVC/2004 no próprio site[1] da competição. A Tabela 4.1 descreve as características particulares dessas 12 bases de imagens.

Tabela 4.1: Base de imagens do *Fingerprint Verification Competition* (FVC) dos anos de 2000, 2002 e 2004.

FVC 2000				
Banco	Forma de Aquisição	Res. da Imagem	Qtd de ID	Qtd de imagens
DB1a e DB1b	*Low-cost Optical Sensor*	300x300	110	8 x 110 = 880
DB2a e DB2b	*Low-cost Capacitive Sensor*	256x364	110	8 x 110 = 880
DB3a e DB3b	*Optical Sensor*	448x478	110	8 x 110 = 880
DB4a e DB4b	*Synthetic Generator*	240x320	110	8 x 110 = 880
FVC 2002				
Banco	Forma de Aquisição	Res. da Imagem	Qtd ID	Qtd de imagens
DB1a e DB1b	*Optical Sensor*	388x374	110	8 x 110 = 880
DB2a e DB2b	*Optical Sensor*	296x560	110	8 x 110 = 880
DB3a e DB2b	*Capacitive Sensor*	300x300	110	8 x 110 = 880
DB4a e DB4b	*SFinGe v2.51*	288x384	110	8 x 110 = 880
FVC 2004				
Banco	Forma de Aquisição	Res. da Imagem	Qtd ID	Qtd de imagens
DB1a e DB1b	*Optical Sensor*	640x480	110	8 x 110 = 880
DB2a e DB2b	*Optical Sensor*	328x364	110	8 x 110 = 880
DB3a e DB3b	*Thermal Sweeping Sensor*	300x48	110	8 x 110 = 880
DB4a e DB4b	*SFinGe v3.0*	288x384	110	8 x 110 = 880
Total de 1320 ID em 10560 imagens				

Cada base de imagens possui um total de 880 imagens, sendo que cada impressão digital é adquirida 8 vezes. Ou seja, 110 impressões digitais distintas são capturadas 8 (oito) vezes. Cada base de imagens é dividida em um subconjunto A com 100 imagens

[1] http://bias.csr.unibo.it/fvc2004/download.asp

e em um subconjunto B com 10 imagens. O subconjunto B fica disponível antes da competição para servir de ajustes para os competidores. No subconjunto A estão as imagens que serão de fato utilizadas na competição.

Estas bases de teste não possuem um número de imagens suficientemente grande para se obter uma avaliação indubitável acerca do desempenho do Sistema em questão. No entanto, se pode ter uma estimativa confiável sobre como o sistema se comporta diante da variabilidade presente nessas bases de testes. Para isso, a organização da competição se preocupou em reproduzir nas bases de teste as mesmas condições que um SB teria no seu uso comercial.

Para ilustrar a preocupação que a organização da FVC teve em retratar fielmente as condições reais, é descrito o processo de Aquisição das imagens das bases de testes do FVC/2000 (MAIO et al., 2002a). O processo de Aquisição das competições FVC/2002 e FVC/2004 estão descritos em (MAIO et al., 2002b) e (MAIO et al., 2004), respectivamente.

As imagens de ID dos bancos DB1 e DB2 do FVC/2000 possuem as seguintes características:

- Os voluntários eram estudantes entre 20 a 30 anos de idade sendo aproximadamente metade de cada sexo;
- De cada voluntário foram coletadas imagens de até 4 ID (dedo médio e indicador de ambas mãos);
- O processo de aquisição foi executado por uma pessoa não treinada, portanto não houve cuidado para garantir a qualidade da ID adquirida;
- Para cada voluntário houve oito sessões distintas para capturar as ID, ou seja, na primeira sessão foi coletada a primeira amostra das ID do voluntário, na segunda sessão foi coletada a segunda amostra das mesmas ID da primeira sessão e assim sucessivamente;
- Não houve preocupação em limpar sistematicamente o dispositivo de aquisição;
- Não houve o cuidado em colocar a digital em uma posição certa, portanto não era garantida a presença de singularidades na imagem capturada;

- Terminado o processo de aquisição, foi realizada uma análise nas imagens capturadas. Foram descartadas as imagens que continham a ID com inclinação fora do intervalo $[-15^o, 15^o]$ e era garantida que entre todas as imagens capturadas de uma digital tivessem alguma área com sobreposição;

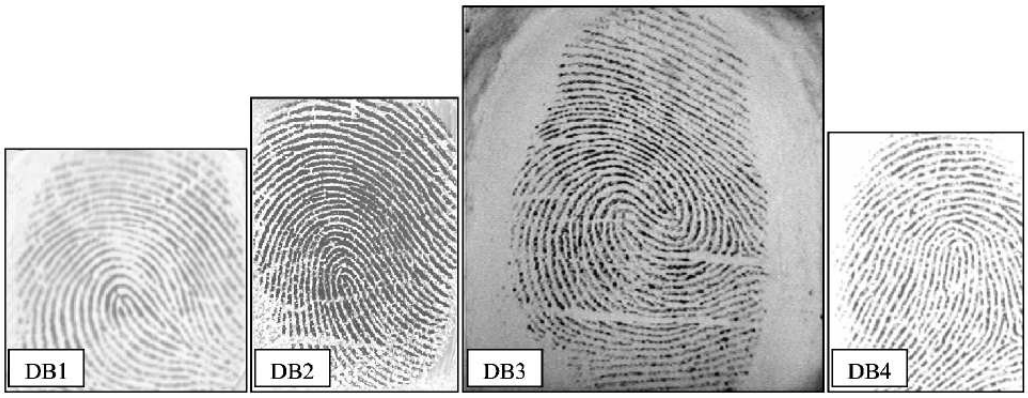


Figura 4.1: Exemplos das imagens da uma ID pertencente a cada base de imagens do FVC/2000.

As imagens de ID do banco DB3 possuem as seguintes características:

- Era um total de 19 voluntários entre 5 a 73 anos de idade, 55% do sexo masculino;
- Um terço dos voluntários tinha mais de 55 anos de idade;
- Um terço dos voluntários tinha menos de 18 anos de idade;
- Um sexto dos voluntários tinha menos de 7 anos de idade (digitais de crianças nesta idade constituem um caso interessante de estudo, pois a área da ID é pequena e a densidade de linha é alta);
- Duas imagens da ID, podendo ser de 1 até 6 dedos (Dedo médio, indicador e polegar de ambas mãos) por voluntário, eram adquiridas em uma mesma sessão totalizando um total de 4 sessões;
- O intervalo entre a primeira sessão e a última sessão variou de 3 dias a 3 meses, dependendo do voluntário;
- O dispositivo de aquisição foi limpo entre cada processo de aquisição;
- Em pelo menos uma sessão os dedos dos voluntários foram limpos com álcool e secados devidamente;

- Terminado o processo de aquisição, foi realizada uma análise nas imagens capturadas. Foram descartadas as imagens que continham a ID com inclinação fora do intervalo $[-15^o, 15^o]$, e era garantida que entre todas as imagens capturadas de uma digital tivessem área com sobreposição;

As imagens das ID do bancos DB4 foram geradas artificialmente pelo aplicativo *(Synthetic Generator)*. É um método barato e rápido de se ter imagens de ID, não há problemas em relação ao direito de privacidade e é possível variar a dificuldade das imagens.

A Figura 4.1 exemplifica as imagens de cada base de dados do FVC/2000 e a Figura 4.2 mostra a variabilidade das imagens de uma mesma ID.

Figura 4.2: Imagens de uma mesma ID capturada em sessões diferentes.

4.3 Critério de Avaliação

Outra contribuição realizada pela competição FVC foi padronizar o critério de avaliação do PRIID. Antes cada pesquisa ou produto comercial apenas destacava a taxa de acerto do seu algoritmo desenvolvido, deixando pouco claro qual foi o procedimento adotado para chegar a essa taxa. Desta forma, a FVC institui um protocolo de avaliação que é descrito a seguir.

Para cada base de dados existem 880 imagens de 110 ID, sendo 800 imagens para a avaliação e 80 imagens destinadas para ajustes. Portanto, para cada banco na base

de imagens há 100 ID distintas. Desta forma o algoritmo de avaliação define a impressão digital como F_{ij} onde i refere-se a i-ésima ID e j como j-ésima amostra da F_i (MAIO et al., 2002a).

Para cada base de dados, o algoritmo de competidor é avaliado quanto a sua Taxa de Erro no Registro (REJ_{reg}), Tempo Médio de Registro (AVG_{reg}), Tamanho Médio do Registro ($SIZE_{reg}$), Taxa de Falsa Aceitação (FAR), Taxa de Falsa Rejeição (FRR), Taxa de Falha na Verificação (REJ_{veri}), Tempo Médio de Verificação (AVG_{veri}) e quanto os erros ERR, $ZeroFAR$ e $ZeroFRR$. Os valores dessas variáveis são determinados pelos seguintes passos:

1. Para todas as imagens das bases de dados I_{ij} $(i = 1 \ldots 100 \; e \; j = 1 \ldots 7)$ o algoritmo do competidor extrai as características correspondes da ID e registra a sua representação como a F_{ij} correspondente. Durante o processo de Representação do competidor podem ocorres três falhas:

   (a) F (Falha do Algoritmo): o algoritmo do competidor declara que não conseguiu processar a imagem I_{ij} e, portanto não há o registro;

   (b) T (Tempo Esgotado): o tempo de registro excedeu ao tempo limite (15 segundos);

   (c) C (Falha na Execução): o algoritmo levantou uma exceção (*crash*) durante a sua execução.

   Todas essas falhas irão compor a Taxa de Erro no Registro (REJ_{reg}). O Tempo de Execução de cada extração de características irá compor o Tempo Médio de Registro (AVG_{reg}).

2. Para todas as representações anteriormente registradas, as oito representações de uma mesma F_i são confrontadas entre si. Isto é, a representação F_{ij} e a $F_{ik}(j < k \leq 8)$ são confrontadas pelo algoritmo de verificação do competidor, a saída do algoritmo é armazenada no vetor gms_{ijk}[2]. Nesta etapa o algoritmo é avaliado quanto ao seu Grau de Falsa Rejeição (FRR), pois neste momento todas as verificações devem ser positivas. Esta etapa é conhecida como Reconhecimento Genuíno. O número de reconhecimento positivo é denotado por $NGRA$[3]. Se a execução do algoritmo

[2] *Genuine Matching Scores.*

[3] *Number of Genuine Recognition Attempts.*

de verificação falhar ou ultrapassar o tempo limite de execução (5 segundos) será considerado como Erro de Verificação. Todos os Erros de Verificação serão computados na Taxa de Erro na Verificação (REJ_{NGRA}).

3. Para cada representação F_{i1} é feita um confronto entre ela e as outras representações $F_{k1}(i < k \leq 100)$. Nesta etapa é avaliado o Grau de Falsa Aceitação. O número de reconhecimento negativo é denotado por NIRA[4]. Como no procedimento anterior, se o algoritmo de verificação falhar ou ultrapassar o tempo limite de execução (5 segundos) será considerado com falha na verificação. Portanto, será registrada na Taxa de Erro na Verificação REJ_{NIRA}. A Taxa de Erro da Verificação Total é igual a $REJ_{veri} = REJ_{NGRA+NIRA}$. A saída do algoritmo de verificação é registrada no vetor ims_{ik}[5]. Esta etapa é conhecida como Reconhecimento Impostor. O tempo de execução de cada processo de verificação dos passos 2 e 3 irá compor o Tempo Médio de Verificação AVG_{veri}.

4. Cada um dos vetores gms_{ijk} e ims_{ik} gera um histograma. É esperado que os valores do vetor gms_{ijk} estejam próximos de 1 (um), pois a verificação atua sobre representações da mesma ID. Portanto deve sempre o ocorrer o reconhecimento positivo. Já no vetor ims_{ik} é esperado que os valores fiquem próximos de 0 (zero), pois só há verificação entre ID diferentes devendo ocorrer sempre o reconhecimento negativo. Desta forma, espera-se que a curva do histograma gerado pelo vetor gms_{ijk} seja crescente, e a curva gerado pelo vetor ims_{ik} seja decrescente.

5. A partir dos vetores gms_{ijk} e ims_{ik} são construídas as curvas $FRR(t)$ e $FAR(t)$ sendo t o limiar que indica o reconhecimento positivo ou negativo. Dado um determinado limiar t que varia de $[0,1]$, a curva $FAR(t)$ denota a porcentagem do elementos do vetor tal que $ims_{ik} \geq t$ e a curva $FRR(t)$ denota a porcentagem dos elementos do vetor $gms_{ijk} < t$. Através da análise dessas curvas é que se obtém uma compreensão do desempenho do algoritmo de verificação. As equações 4.1 e 4.2 definem a construção das curvas $FAR(t)$ e $FRR(t)$.

$$FAR(t) = \frac{num.elementos\{ims_{ik} | ims_{ik} \geq t\}}{NIRA} \tag{4.1}$$

[4] *Number of Impostor Recognition Attempts.*

[5] *Impostor Matching Scores.*

$$FRR(t) = \frac{num.elementos\{gms_{ijk} | gms_{ijk} < t\} + REJ_{NGRA}}{NGRA} \tag{4.2}$$

6. Outras medidas úteis na para avaliação de um algoritmo de verificação são os erros *EER*, *ZeroFAR* e *ZeroFRR* (Ver seção 2.1.3.1). O *ERR* é o erro computado no ponto t tal que $FAR(t) = FRR(t)$, o seu valor é obtido de acordo com as equações 4.5 e 4.6 .O *ZeroFAR* e o *ZeroFRR* são determinados pelas equações 4.7 e 4.8, respectivamente. Nota-se que caso essa equações não retornem nenhum valor, o *ZeroFAR* e o *ZeroFRR* recebem o valor igual a 1 (um) (MAIO et al., 2002a).

$$t_1 = max\{t | FRR(t) \leq FAR(t)\} \tag{4.3}$$

e

$$t_2 = min\{t | FRR(t) \geq FAR(t)\} \tag{4.4}$$

$$[EER_{low}, EER_{high}] = \begin{cases} [FRR(t_1), FAR(t_1)] & \text{se} \quad FRR(t_1) + FAR(t_1) \leq FAR(t_2) + FRR(t_2) \\ [FAR(t_2), FRR(t_2)] & \text{caso contrário} \end{cases} \tag{4.5}$$

$$EER_{estimado} = \frac{(ERR_{low} + ERR_{high})}{2} \tag{4.6}$$

$$ZeroFAR(t) = min\, t\{FRR(t) | FAR(t) = 0\} \tag{4.7}$$

$$ZeroFRR(t) = min\, t\{FAR(t) | FRR(t) = 0\} \tag{4.8}$$

As métricas discutidas nos parágrafos anteriores avaliam o processo de verificação. Quanto ao processo de extração de características as métricas utilizadas são a Taxa de Acerto (TA), Taxa de Falsa Extração Positiva (TFEP) e a Taxa de Falsa Extração Negativa (TFEN). A primeira medida diz respeito ao percentual calculado pelo número de extrações de características corretas sobre o total de informações extraídas. A segunda é o número de extrações incorretas sobre total de informações extraídas e a última medida é o número de características não extraídas sobre o total de características existentes. A

seção seguinte expõe os resultados tanto do processo de extração de características quanto do processo de verificação.

4.4 Resultados Obtidos

Esta seção apresenta os resultados de todos os processos implementados neste trabalho. Na primeira subseção é apresentado os resultados do processo de extração de características, que na verdade corresponde as extrações de singularidades, de minúcias e número de linhas (cristas) entre dois pontos. Na segunda subseção é a vez da apresentação dos resultados do processo de verificação. Além das métricas comentadas na seção anterior, os resultados são acompanhados por estatísticas das informações extraídas e do tempo consumido. Alguns resultados são ilustrados e comentados. Para efeito de análise do tempo consumido, todos os testes foram executados em um computador com processador Pentium IV 3.2GHz HT com 2Gbytes de RAM.

4.4.1 Extração de Características

4.4.1.1 Singularidades

Como visto na seção 3.2.3.2, foram implementados dois métodos de extração de singularidades: o método baseado no índice de Poincaré extraído do campo direcional e o método baseado na proposta de Jain et al. (2000). Ambos receberam como argumento a imagem da ID após aplicação do filtro de Gabor Neural proposto por Marques (2004). Para avaliar o resultados de ambos os métodos, foi construído um aplicativo que auxiliou a marcação manual das singularidades da ID. Para cada marcação este aplicativo registrava a coordenada (x,y) e o tipo da singularidade. Vale ressaltar que esta marcação não foi realizada por um perito papiloscopista. Os resultados dos métodos implementados são comparados com os dados desta marcação manual.

A fim de obter uma avaliação sobre os métodos foram consolidadas três informações: estatísticas sobre a quantidade de singularidades extraídas, estatísticas sobre o tempo da extração de singularidades e taxas de acerto e de erro da extração de singularidades. A Tabela 4.2 mostra as quantidades de singularidades extraídas pela Marcação Manual, pelo Método Índice de Poincaré e pelo Método de Jain et al. (2000) para o banco DB1 do FVC/2000. Vale ressaltar que este último método só extrai singularidades do tipo Núcleo.

Tabela 4.2: Estatísticas sobre a quantidade de singularidades extraídas pela marcação manual, Índice de Poincaré e Gabor - Base de Imagens DB1/FVC2000.

	Marcação Manual			Método Índice de Poincaré			Método Jain et al. (2002)
	Núcleo	Delta	Ambos	Núcleo	Delta	Ambos	Núcleo
Média	1.04	0.18	1.22	1.59	1.00	2.59	1.00
Mediana	1.00	0.00	1.00	1.00	1.00	2.00	1.00
Mínimo	0.00	0.00	0.00	0.00	0.00	0.00	1.00
Máximo	4.00	2.00	4.00	7.00	5.00	12.00	1.00
Desvio Padrão	0.76	0.42	0.89	0.94	0.97	1.64	0.00
Total	915	155	1070	1402	881	2283	880

Tabela 4.3: Estatísticas sobre o tempo consumido no processo de extração de singularidade pelo método Índice de Poincaré e de Jain et al. - Base de Imagens DB1/FVC2000.

	Método Índice de Poincaré	Método de Jain et al.(2002)
Média	0.6857s	0.8539s
Mediana	0.6870s	0.8590s
Mínimo	0.5930s	0.8120s
Máximo	0.7190s	1.7030
Desvio Padrão	0.0156s	0.0315s
Total	603.4120s	751.4350s

Já a Tabela 4.3 mostra as estatísticas sobre o tempo consumido em cada método para o banco DB1 do FVC/2000. Com essas informações é possível avaliar se os métodos implementados podem ser usados em aplicativos que exijam pequeno tempo de resposta. Por fim, a Tabela 4.4 apresentam o desempenho dos métodos implementados. O critério da avaliação dos métodos foi o seguinte:

1. Todas as singularidades $(SING_e)$ extraídas de uma ID pelo o método a ser avaliado são comparadas com as singularidades $(SING_m)$ da marcação manual de uma ID. Se o tipo da $SING_e$ for igual ao tipo da $SING_m$ e a distâncias entre elas for menor Δs então será considerada como extração CORRETA senão extração INCORRETA POSITIVO. Nota-se que se duas $(SING_e)$ estiverem próximas de uma única $(SING_m)$ ambas serão consideradas corretas;

2. Todas as singularidades $(SING_m)$ da marcação manual de uma ID são comparadas com as singularidades $(SING_e)$ extraídas de uma ID pelo método a ser avaliado. Se o tipo da $SING_m$ for igual ao tipo da $SING_e$ e a distâncias entre elas for menor que

um Δs específico então será considerada como extração *CORRETA* senão extração INCORRETA NEGATIVO. Caso não haja nenhuma $SING_e$, ocorrerá também uma extração INCORRETA NEGATIVO;

3. Taxa de Acerto é igual ao número de extração CORRETA sobre a soma das quantidades $SING_e$ e quantidade $SING_m$;

4. Taxa de Falsa Extração Positiva é igual ao número de extração INCORRETA POSITIVA sobre a quantidade de $SING_e$;

5. Taxa de Falsa Extração Negativa é igual ao número de extração INCORRETA NEGATIVA sobre a quantidade de $SING_m$;

Tabela 4.4: Resultado do processo de extração de singularidades para distância máxima de 10, 20 e 30 Pixels - Índice de Poincaré - Base de Imagens FVC2000/DB1.

	Índice de Poincaré			Proposto por Jain et al. (2000)		
	Δs $10 pixels$	Δs $20 pixels$	Δs $30 pixels$	Δs $10 pixels$	Δs $20 pixels$	Δs $30 pixels$
Detecção Positiva	564 $24,70\%$	912 $39,95\%$	991 $43,41\%$	530 $60,23\%$	612 $69,55\%$	627 $71,25\%$
Detecção Falsa-Positiva	1719 $75,30\%$	1371 $60,05\%$	1292 $56,59\%$	350 $39,77\%$	268 $30,45\%$	253 $28,75\%$
Detecção Falsa-Negativa	474 $44,30\%$	118 $11,03\%$	54 $5,04\%$	538 $50,28\%$	452 $42,24\%$	436 $40,75\%$

A partir dos dados da tabela 4.2, percebe-se que o método do Índice do Poincaré detecta um quantidade de singularidade do tipo Delta bem superior a quantidade aferida pela marcação manual. Por conseqüência, subentende-se que este método não possui uma boa acurácia na detecção da singularidade do tipo Delta. Fato esse, que pode explicar a baixa taxa de acerto apresentada na Tabela 4.4. A fim de descobrir a razão deste mau desempenho, foi feita uma averiguação nas ID que continham mais singularidades do tipo Deltas detectadas. A Figura 4.3 ilustra um exemplo dessas ID, esta figura é composta da imagem bruta, a imagem com filtro de Gabor e o campo direcional com as singularidades detectadas das ID (Quadrado Cinza Escuro - Núcleo e Quadrado Branco - Delta).

Portanto, pelas as imagens da Figura 4.3 nota-se que o campo direcional nas regiões de contorno da imagem após o filtro de Gabor geram configurações que o índice

(a) Imagem Bruta (b) Imagem após o Filtro de Gabor (c) Campo Direcional com as Singularidades

Figura 4.3: Extração de singularidades da ID com saior número de singularidades 7 (sete) do tipo Núcleo e 5 (cinco) do Tipo Delta.

de Poincaré avalia erroneamente com uma singularidade. Isto é, certas regiões no interior da ID são segmentadas como se não fossem parte de ID, por isso os buracos brancos na ID com filtro de Gabor. Na ID retratada na Figura 4.3 há dois núcleos, ambos foram corretamente detectados. Mas, as regiões de borda geraram 7 (sete) extrações falsas positivo. Para tanto, foi avaliado o desempenho da extração de cada tipo de singularidade. As Tabelas 4.5 e 4.6) apresentam os resultados separados pelo tipo de singularidade. Pelos dados dessa tabela é perceptível que o método de índice de Poincaré há uma grande ocorrência de falso positivo e baixa ocorrência de falso negativo. Nota-se também que detecção da singularidade do tipo Núcleo tem melhor desempenho que a detecção da singularidade do tipo Delta.

Tabela 4.5: Resultado do processo de extração de singularidades para distância máxima de 10, 20 e 30 Pixels - Índice de Poincaré - Base de Imagens FVC2000/DB1 - Somente singularidade do Tipo Núcleo.

	Índice de Poincaré - Somente Núcleo		
	$\Delta s = 10 pixels$	$\Delta s = 20 pixels$	$\Delta s = 30 pixels$
Detecção Positiva	453 32,31%	769 54,85%	847 60,41%
Detecção Falsa-Positiva	949 67,67%	633 45,15%	555 39,59%
Detecção Falsa-Negativa	436 47,65%	116 12,67%	53 5,79%

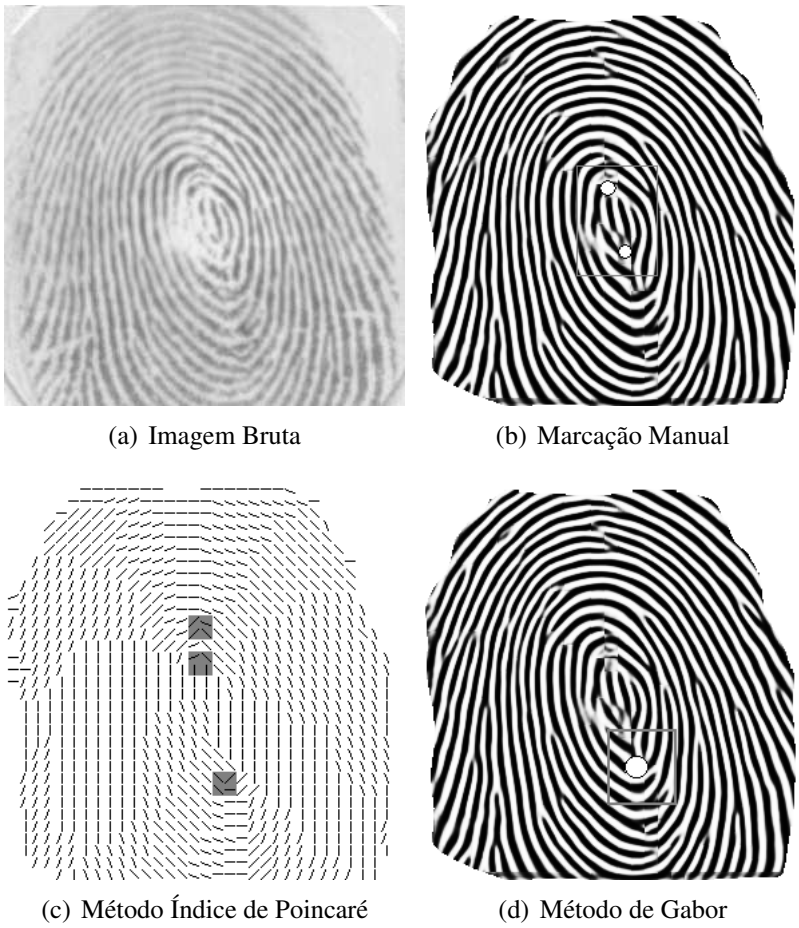
Em relação ao tempo consumido, o método de Índice de Poincaré possui uma duração menor que o proposto por Jain et al. (2000) (Ver Tabela 4.3). Contudo, este

Tabela 4.6: Resultado do processo de extração de singularidades para distância máxima de 10, 20 e 30 Pixels - Índice de Poincaré - Base de Imagens FVC2000/DB1 - Somente singularidade do tipo Delta.

	Índice de Poincaré - Somente Delta		
	$\Delta s = 10 pixels$	$\Delta s = 20 pixels$	$\Delta s = 30 pixels$
Detecção Positiva	111 12,60%	143 16,23%	144 16,35%
Detecção Falsa-Positiva	770 87,40%	738 83,77%	737 83,65%
Detecção Falsa-Negativa	38 24,51%	2 1,29%	1 0,65%

último pode ser aplicado a uma imagem bruta sem grandes perdas no desempenho. Sendo assim, se for levado em conta o tempo gasto na aplicação do filtro de Gabor, o método que usa o índice de Poincaré consumiria mais tempo. O fato de só detectar singularidade do tipo Núcleo é um ponto negativo ao método de Jain et al. (2000). Por fim, considerando que marcação manual seja uma marcação correta conclui-se que o método de índice de Poincaré tem um desempenho razoável no que tange a extração de singularidade do tipo Núcleo. Dificilmente, este método deixa de detectar a singularidade, visto o baixo valor da Taxa de Falso Negativo. No entanto, é fortemente dependente da qualidade da imagem. Já o método proposto por Jain et al. (2000) é mais robusto, ou seja, não dependente tanto da qualidade da imagem quanto o método anterior. Era esperado que o método de Jain et al. (2000) tivesse um melhor desempenho. Para tanto, analisou-se alguns exemplos onde este método falhou.

As imagens da Figura 4.4 mostra a imagem bruta e as posição da singularidades feitas pela marcação manual, pelo método índice de Poincaré e o pelo método de Jain et al. (2000). Percebe-se que neste caso, este último método teria marcado erroneamente uma singularidade se a marcação manual fosse considerada como a posição correta. Mas, pela imagem de ID fica difícil determinar a posição ideal da singularidade do tipo núcleo. Logo, não é possível tecer comentários confiáveis acerca das Taxa de Acerto, de Marcação Falso-Negativa ou Falso-Positiva sobre os métodos de extração de singularidades implementados.



(a) Imagem Bruta (b) Marcação Manual

(c) Método Índice de Poincaré (d) Método de Gabor

Figura 4.4: Posição da singularidade do tipo Núcleo pela marcação manual, método de índice de Poincaré e método de Jain et. al (2000).

4.4.1.2 Minúcias

Ao longo deste trabalho, foi amplamente exposto que as minúcias são as principais características identificadoras de uma ID. Afirmativa essa que é provada pelo fato que a maioria dos SB baseados em ID usa minúcias como os descritores identificadores (MALTONI et al., 2003). Logo, o desempenho do processo de extração de minúcias implica fortemente no desempenho do PRIID como um todo.

Entretanto, avaliar o desempenho do processo de extração de minúcias não é uma tarefa simples. Localizar uma minúcia em uma imagem de ID de boa qualidade é fácil, mas em uma ID com muito ruído é bem possível localizar uma minúcia erroneamente. Da mesma forma que foi feita na extração de singularidades, a Tabela 4.7 e 4.8 mostram, respectivamente, as estatísticas sobre a quantidade de minúcias extraídas e sobre o tempo de processamento. Vale a pena lembrar, que somente o tempo do método clássico de extração, discorrido na Seção 3.2.3.3, foi computado. Outros dados importantes são a Taxa

de Erro de Registro (REJ_{reg}) e a Tamanho Médio do Registro ($SIZE_{reg}$). Sobre o banco DB1 do FVC de 2000, o método proposto por Marques (2004) gerou 11 falhas no registro ($REJ_{reg} = 1,25\%$) e no método clássico houve uma falha no registro ($REJ_{reg} = 0,11\%$). E o Tamanho Médio do arquivo onde ficam armazenadas as minúcias é igual a kbytes $SIZE_{reg} = 5Kbytes$.

Tabela 4.7: Estatísticas sobre a quantidade de minúcias extraídas pelo método proposto por Marques (2004) e pelo método clássico implementado - Base de Imagens DB1/FVC2000.

	Método Marques(2004)			Método Clássico		
	Bifurcação	Terminação	Ambos	Bifurcação	Terminação	Ambos
Média	18.68	18.23	36.92	20.19	22.17	42.37
Mediana	18.00	18.00	36.00	19.00	22.00	42.00
Mínimo	3.00	1.00	13.00	1.00	2.00	9.00
Máximo	47.00	50.00	73.00	57.00	69.00	96.00
Desvio Padrão	6.33	7.69	10.11	7.19	8.48	12.70
Total	16086	15701	31789	17751	19495	37246

Não foi feita nenhuma marcação manual das minúcias como foi feita para as singularidades. A marcação da posição (x,y) e do ângulo da minúcia em todas ID seria uma tarefa extremamente dispendiosa. Desta forma, para cada base de imagens foram escolhidas cinco imagens. O critério de avaliação da extração de minúcias é similar ao de singularidade e é composto pelos seguintes passos:

1. Todas as minúcias ($MINU_e$) extraídas de uma ID pelo método a ser avaliado são comparadas com as minúcias ($MINU_m$) reais de uma ID. Se o tipo da $MINU_e$ for igual ao tipo da $MINU_m$, a distância entre elas for menor Δs e a diferença entre as direções das minúcias for menor que um $\Delta\theta$ específico, então extração CORRETA senão extração INCORRETA POSITIVO;

2. Todas as minúcias ($MINU_m$) reais de uma ID são comparadas com as minúcias ($MINU_e$) extraídas de uma ID pelo método a ser avaliado. Se o tipo da $MINU_m$ for igual ao tipo da $MINU_e$, as distâncias entre elas for menor que Δs e a diferença entre as direções das minúcias for menor $\Delta\theta$, então extração CORRETA senão extração INCORRETA NEGATIVO;

3. Taxa de Acerto é igual ao número de extração CORRETA sobre a quantidade $MINU_e$;

4. Taxa de Falsa Extração Positiva é igual ao número de extração INCORRETA POSITIVA sobre a quantidade de $MINU_e$;

5. Taxa de Falsa Extração Negativa é igual ao número de extração INCORRETA NEGATIVA sobre a quantidade de $MINU_m$;

Tabela 4.8: Estatísticas sobre o tempo consumido no processo de extração de minúcias pelo método clássico - Base de Imagens DB1/FVC2000.

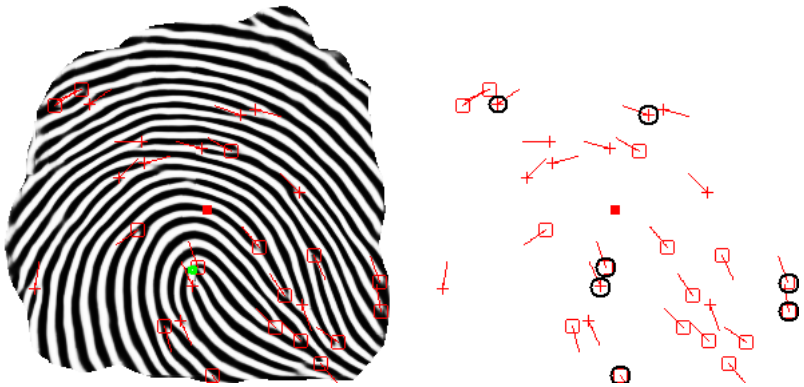
	Método Clássico
Média	$1.80s$
Mediana	$1.78s$
Mínimo	$1.55s$
Máximo	$2.75s$
Desvio Padrão	$0.12s$
Total	$1582s$

A Tabela 4.9 mostra o resultado do processo de extração de minúcias para uma imagem. Vale ressaltar que a medição da distância e o processo de validação das minúcias são tarefas complicadas. Percebe-se que de modo geral ambos os métodos extraíram corretamente as minúcias, entretanto em alguns casos houve inversão quanto ao tipo de minúcia, isto é, a validação do processo de extração de minúcias fica prejudicada por não existir uma base de dados com as minúcias corretas. As Figuras 4.5, 4.6 e 4.7 ilustram a dificuldade em validar o processo de extração de minúcias. As minúcias envolvidas por um círculo são as minúcias espúrias. Não foi avaliado o ângulo e o tipo das minúcias somente a sua posição.

Tabela 4.9: Resultado do processo de extração de minúcias.

	Por Filtro de Gabor (MARQUES, 2004)	Método Clássico
Detecção Positiva	21 75,00%	21 77,78%
Detecção Falsa-Positiva	7 25,00%	6 22,22%
Detecção Falsa-Negativa	0 0,00%	0 0,00%

Figura 4.5: A imagem bruta da ID onde foi validado a extração de minúcias. Nota-se a dificuldade em determinar os dados relativos as minúcias.



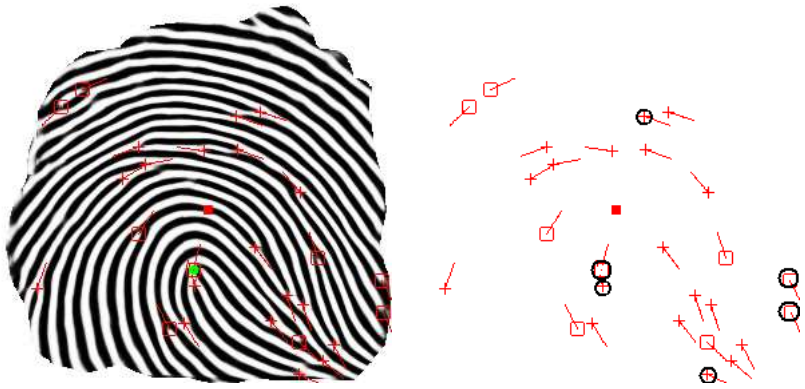
(a) Imagem e Minúcias (b) Só as Minúcias

Figura 4.6: Extração de minúcias proposto por Marques (2004). As minúcias envolvidas por um círculo foram consideradas como minúcias espúrias

4.4.1.3 Outras Características

Além das singularidades e das minúcias, outras informações como as distâncias entre as minúcias; as distâncias entre as minúcias e o centróide da imagem; as distâncias entre as minúcias e as singularidades; a matriz de características locais e o número de linhas entre dois pontos são também utilizadas nos métodos de verificação implementados. Foi computado o tempo gasto para cada extração dessas informações.

O Tempo Médio de Registro (AVG_{reg}) será composto pelo tempo gasto na



(a) Imagem e Minúcias (b) Só as Minúcias

Figura 4.7: Extração de minúcias pelo método Clássico. As minúcias envolvidas por um círculo foram consideradas como minúcias espúrias

extração dessas informações mais o tempo consumido pela extração das minúcias e das singularidades. A Tabela 4.10 mostra o tempo gasto no cálculo das distâncias e do centro de massa da imagem e da construção da matriz de características locais. A coluna Conjunto 1 indica que as características locais foram baseadas nas minúcias extraídas pelo método de Marques (2004) e a coluna Conjunto 2 foram baseadas nas minúcias extraídas pelo método clássico.

Tabela 4.10: Estatísticas sobre o tempo consumido no cálculo das distâncias e na construção da matriz de características locais - Base de Imagens DB1/FVC2000.

	Cálculo das Distâncias e do Centróide	Construção da Matriz de Características Locais	
		Conjunto 1	Conjunto 2
Média	0.005s	0.386s	0.413s
Mediana	0.000s	0.390s	0.406s
Mínimo	0.000s	0.141s	0.109s
Máximo	0.016s	0.768s	1.078s
Desvio Padrão	0.007s	0.100s	0.114s
Total	4.460s	333.446s	362.610s

Logo, somando o tempo gasto na extração de todas as características chega-se ao Tempo Médio de Registro (AVG_{reg}) igual a soma do tempo de extração de minúcias, tempo de extração de singularidades, tempo de cálculo das distâncias e do centróide e o tempo da construção da matriz de características locais. Assumindo os valores médios de cada tarefa, pelas Tabelas 4.8, 4.3 e 4.10, o Tempo Médio de Registro (AVG_{reg}) seria igual

a $(1.80+0.854+0.005+0.413) = 3.072s$. Vale ressaltar que cada método de verificação utiliza um subconjunto dessas informações extraídas e o tempo do aprimoramento da imagem pelo filtro de Gabor não foi computado.

Junto com a medição do desempenho da extração de minúcias também foi feita a análise da extração do número de linhas (cristas) entre duas minúcias. Aferiu-se que a extração de número de linhas (cristas) possui um bom desempenho, apresentando em apenas alguns casos de erro de contagem de duas linhas a mais ou a menos.

4.4.2 Verificação

Como visto na seção 3.2.4.4, foram implementados quatro métodos de verificação: o Método do Centróide, o Método Exaustivo, o Método da Singularidade e o Método Características Locais. Todos esses métodos utilizam as minúcias como características identificadoras. O Método do Centróide além das minúcias utiliza a coordenada do centro de massa da imagem. O Método da Singularidade usa as coordenadas das singularidades e quando não as possui usa a coordenada do centro de massa da imagem. O Método Características Locais usa a matriz de características locais extraída conforme exposto na seção 3.2.4.4. Já o Método Exaustivo usa apenas as minúcias.

Todos os métodos foram testados de acordo com o critério exposto na seção 4.3. Cada método usou tanto o conjunto de minúcias extraídas pelo processo proposto por Marques (2004) quanto o conjunto de minúcias extraídas pelo método clássico implementado neste trabalho (Ver Seção 3.2.3.3). Para cada associação entre o método de verificação e o conjunto de minúcias foram feitos 4 testes, sendo que no 1º teste os parâmetros de verificação foram iguais a $n = 12$, $\Delta s = 10$ *e* $\Delta\theta = 10$, no 2º teste os parâmetros foram iguais a $n = 12$, $\Delta s = 20$ *e* $\Delta\theta = 20$, e assim sucessivamente, incrementando 10 unidades nos parâmetros Δs *e* $\Delta\theta$ até chegar ao 4º teste com os parâmetros iguais a $n = 12$, $\Delta s = 40$ *e* $\Delta\theta = 40$. Os testes são denominados pelo formato TESTE{METODO}{NUMERO}{LETRA}, o número indica o conjunto de minúcias usadas (1-Gabor e 2-Clássico) e a letra indica os parâmetros (A-$\Delta s = 10$ *e* $\Delta\theta = 10$, ..., D-$\Delta s = 40$ *e* $\Delta\theta = 40$). Desta forma, foi realizado um total de 32 testes sobre o conjunto de imagens DB1 do FVC/2000, esses resultados estão nos apêndices B a E.

Os resultados incluem estatísticas sobre o resultado (Grau de Similaridade)[6]

[6]Termo em português equivalente a palavra inglesa *score*

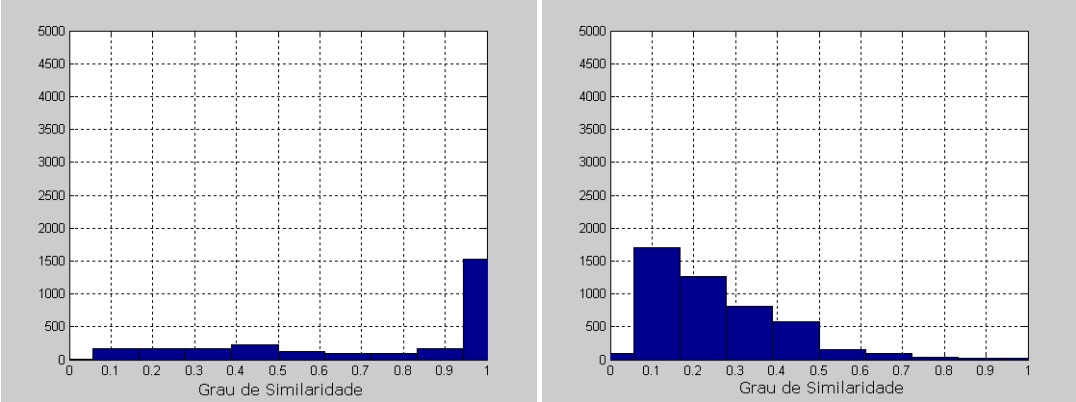
alcançado pelo algoritmo de verificação, número de minúcias equivalentes e o tempo de processamento da verificação. Bem como as métricas definidas na seção 4.3, os histogramas do reconhecimento genuíno e impostor e as curvas $FAR(t)$ e $FRR(t)$. De todos os 32 testes, o TESTECAR.LOCAIS2C foi considerado como o melhor resultado. Baseado nos valores EER, poder-se-ia escolher o TESTECAR.LOCAIS2C ou o TESTECAR.LOCAIS2D como o teste de melhor desempenho. Contudo, preferiu-se escolher o primeiro pelo fato deste possuir uma melhor separação entre o histograma do reconhecimento genuíno e o histograma do reconhecimento impostor. Para o TESTECARAC.LOCAIS2C, a Tabela 4.11 apresenta as estatísticas do processo de verificação, a Figura 4.8 mostra os histogramas do reconhecimento genuíno e impostor e a Figura 4.9 ilustra as curvas $FAR(t)$ e $FRR(t)$.

Tabela 4.11: Resultados sobre o processo de verificação utilizando o método Características Locais com o parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$.

TESTECARAC.LOCAIS2C			
	Reconhecimento Genuíno		
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
Média	0.77	14.34	0.05s
Mediana	1.00	14.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	47.00	1.14s
Desvio Padrão	0.31	8.09	0.08s
	Reconhecimento Impostor		
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
Média	0.27	4.41	0.05s
Mediana	0.25	4.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	18.00	0.55s
Desvio Padrão	0.16	2.01	0.05s
$REJ_{veri} = 0.00$	$EER = 0.19$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

Pelos resultados obtidos nos 32 testes, que estão apresentados nos Apêndices B a E, observou-se que o método de verificação que envolve as características locais combinado com o método clássico de extrações de minúcias obteve o melhor desempenho. Logo, para as demais bases de imagens só será processada a verificação utilizando este método como os parâmetros iguais a $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$. Para assim, ser comparado como os outros algoritmos competidores do FVC. Mas antes, é feito alguns

comentários sobre os resultados desta bateria de testes.



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura 4.8: Histogramas do grau de similaridade do TESTECAR.LOCAIS2C.

Espera-se de qualquer método de verificação que ele retorne um valor próximo de 1 (um) quando duas imagens da mesma ID são a ele submetidas, e um valor próximo de 0 (zero) no caso de duas imagens de ID distintas. Logo, o histograma do reconhecimento genuíno deve se concentrar em valores próximos de 1 (um) e o histograma do reconhecimento impostor em valores próximo de 0 (zero). Ou seja, um histograma deve estar bem distante do outro. Entretanto, os resultados obtidos nos testes não atingiram o desejado. Existe uma grande interseção entre histogramas genuíno e impostor. Fato esse que explica o número alto do *ERR*.

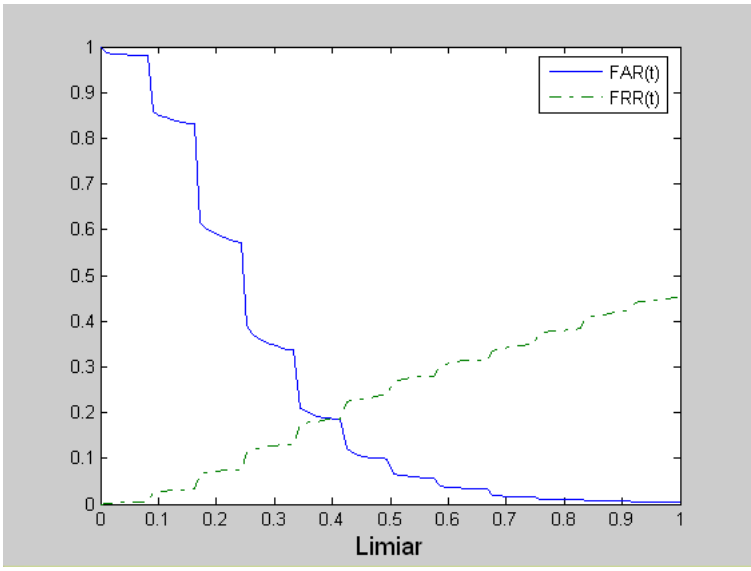


Figura 4.9: Curva FAR(t) e curva FRR(t) do TESTECAR.LOCAIS2C.

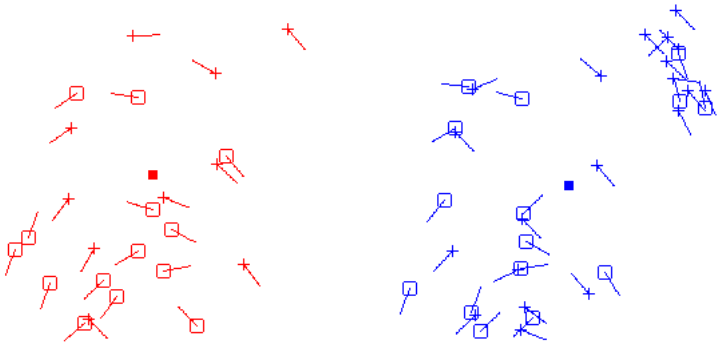
Outra questão negativa a respeito dos resultados, é a alta ocorrência do grau de similaridade igual a 1 no Reconhecimento Impostor. Isto é, sempre há um caso de comparação de ID distintas que retorne o grau de similaridade igual a 1 (um). Logo, uma comparação que deveria retornar negativa é avaliada como uma comparação positiva no seu grau máximo. Isto é medido pelo valor *ZeroFAR*. Somente para parâmetros Δs e $\Delta\theta$ pequenos é que o *ZeroFAR* assume valores abaixo de 1 (um). A situação contrária é pior. Ou seja, praticamente para todos os testes o valor *ZeroFRR* se encontra próximo de 1. Isto que dizer que não importa o método ou os parâmetros, há sempre duas imagens da mesma ID que são avaliadas como se fossem distintas no seu grau máximo (grau similaridade igual a zero). Para tentar explicar esta situação, os exemplos a seguir mostram uma verificação de duas imagens da mesma ID que retornou o grau de similaridade igual a 0 (zero) e um verificação de duas imagens distintas que retornou valor igual a 1 (um).

(a) Bruta 1 (b) Bruta 2

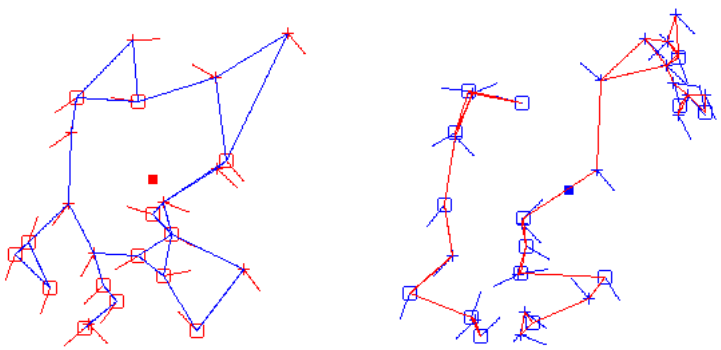
(c) Gabor 1 (d) Gabor 2

Figura 4.10: As imagens brutas e após o filtro de Gabor de ID da mesma pessoa que o processo de verificação avaliou com o grau de similaridade igual a zero.

A Figura 4.10 mostra duas imagens da mesma ID que foram avaliadas pelo processo de verificação como se fossem duas ID distintas com o grau de similaridade igual a zero. Note-se pelas as imagens que elas são da mesma ID, entretanto a imagem 2 retrata mais a parte superior da ID, enquanto a imagem 2 mostra mais a região central da imagem. Já a Figura 4.11(b) ilustra que na imagem 2 foram extraídas muitas minúcias falsas na parte superior à direita devido a mau resultado do filtro de Gabor. Por fim, a Figura 4.12 mostra que as duas minúcias equivalentes escolhidas pela distância do vetor de características na verdade não são a mesma minúcia. Portanto, como apresentado nesta mesma Figura 4.12(b) a transformação linear é baseada em uma translação e rotação equivocada, o que gera nenhuma minúcia coincidente. Por conseqüência o grau similaridade resultante é igual a zero.



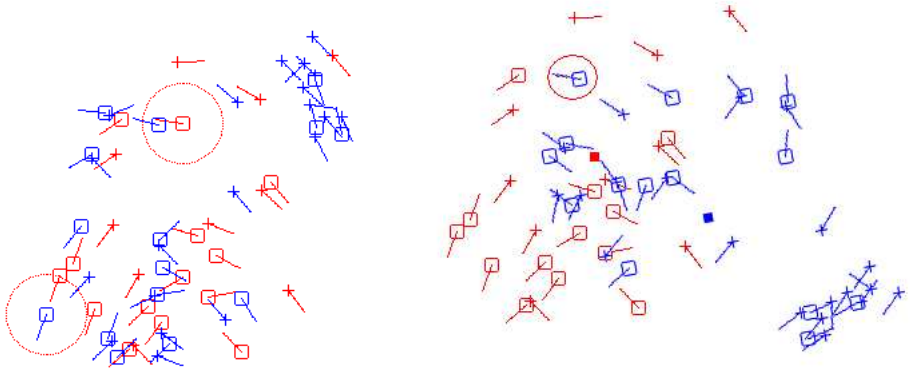
(a) Minúcias 1 (b) Minúcias 2



(c) Características Locais 1 (d) Características Locais 2

Figura 4.11: Minúcias e as indicações das 2 minúcias vizinhas mais próximas da imagem 1 e 2.

A Figura 4.13 mostra duas imagens de duas ID distintas que foram avaliadas pelo processo de verificação como se fossem duas ID iguais com o grau de similaridade



(a) Sobreposição dos conjuntos de minúcias

(b) Transformação Linear sobre o conjunto de minúcias 4

Figura 4.12: O conjunto de minúcias 1 e 2 sobrepostas antes e depois da transformação linear

igual a um. Nota-se pelas imagens que as ID são bem parecidas e que à vista de olhos não treinados poderiam ser consideradas como imagens de uma mesma ID. A Figura 4.14(a) ilustra que na imagem 3 foram extraídas muito mais minúcias que na imagem 4. A região central da imagem 3 existem muitas falsas minúcias. Por fim, a Figura 4.15 mostra que as duas minúcias equivalentes escolhidas pela distância do vetor de características estão localizada no centro da imagem, e portanto, a transformação linear aplicou um pequena translação e rotação. Devido ao $\Delta s = 30$ e $\Delta\theta = 30$ houve muitas minúcias equivalentes (círculos na Figura 4.15), portanto um falso reconhecimento positivo.

Outra observação feita sobre as tabelas dos Apêndices B a E, é que o grau de similaridade do reconhecimento genuíno tende apresentar um desvio padrão maior que no reconhecimento impostor. Logo, pode-se afirmar que o principal problema do processo de verificação é aferir o reconhecimento positivo. No que tange aos parâmetros, percebe-se que uma tolerância pequena faz com que poucos processos de verificação retornem valores próximos de 1 (um). Em relação ao tempo de processamento da verificação AVG_{veri}, os resultados mostram que os métodos de verificação implementados (Seção 3.2.4.4) podem ser utilizados em sistemas comerciais. Com exceção do método exaustivo que se mostrou muito lento.

A seguir é apresentada uma comparação entre melhor método implementado - Método de Verificação pelas Características Locais - e os algoritmos dos competidores do FVC de 2000, 2002 e 2004. Mais dados sobre os algoritmos dos competidores estão

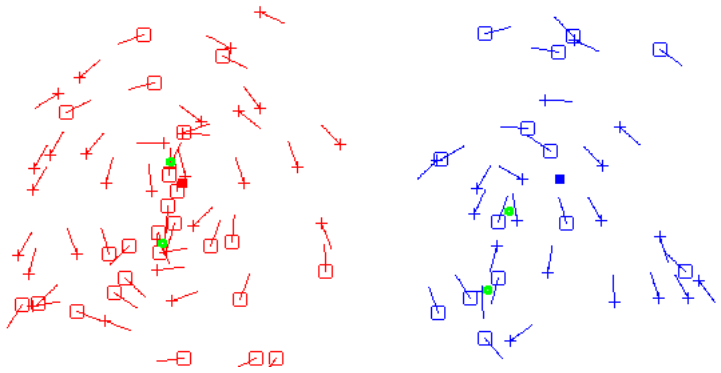
(a) Bruta 3 (b) Bruta 4

(c) Gabor 3 (d) Gabor 4

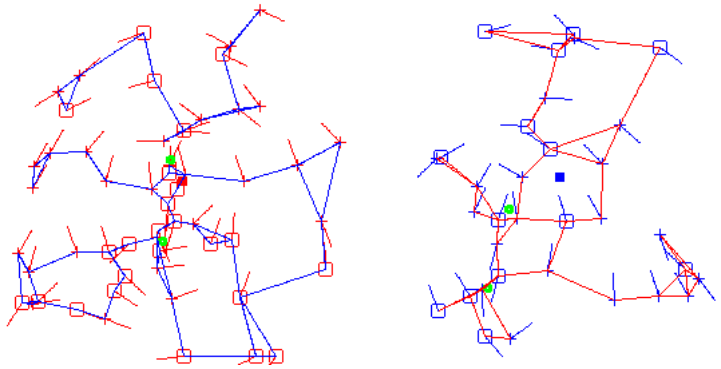
Figura 4.13: As imagens brutas e após o filtro de Gabor de ID distintas que o processo de verificação avaliou com o grau de similaridade igual a 1 (um).

Tabela 4.12: Resultados do DB1 - FVC/2000

Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
Sag1	0.67	0.00	0.00	2.48	0.96
Sag2	1.17	0.00	0.00	0.88	0.88
Cetp	5.06	0.00	0.00	0.81	0.89
Cwai	7.06	3.71	3.90	0.22	0.32
Cspn	7.60	0.00	0.00	0.17	0.17
Utwe	7.98	0.00	0.00	10.40	2.10
Krdl	10.66	6.43	6.59	1.00	1.06
Fpin	13.46	0.00	0.00	0.83	0.87
Unih	21.02	1.71	5.08	0.53	0.56
Diti	23.63	0.00	0.00	0.65	0.72
Ncmi	49.11	0.00	0.12	1.13	1.34
IDSDK	19.00	0.12	0.00	3.07	0.05

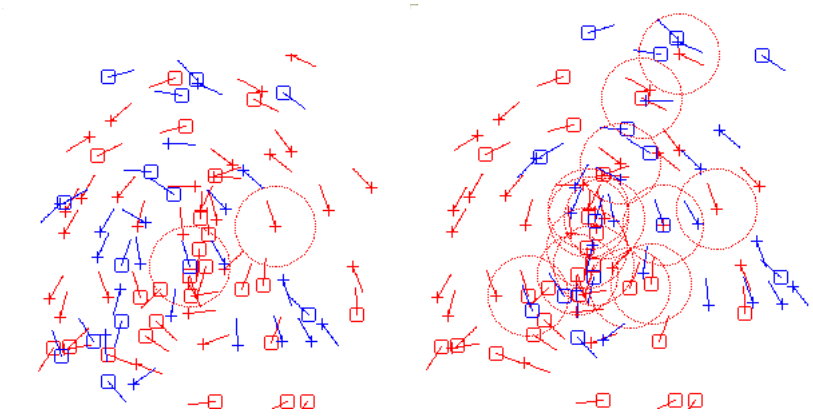


(a) Minúcias 3 (b) Minúcias 4



(c) Características Locais 3 (d) Características Locais 4

Figura 4.14: Minúcias e as indicações das 2 minúcias vizinhas mais próximas da imagem 1 e 2.



(a) Sobreposição dos conjuntos de minúcias (b) Transformação Linear sobre o conjunto de minúcias

Figura 4.15: O Conjunto de minúcias 3 e 4 sobrepostas antes e depois da transformação linear

nos artigos do FVC (MAIO et al., 2002a), (MAIO et al., 2002b) e (MAIO et al., 2004). A Tabela 4.12 mostra o resultados dos algoritmos do FVC/2000 sobre o banco DB1. Na

última linha desta tabela, identificado pelo nome IDSDK está o resultado atingido pelo protótipo implementado. Nota-se que baseado no valor de EER, o método implementado ficou bem longe do melhor resultado, porém houve três algoritmos que obtiveram pior resultado que o IDSDK. Em relação às rejeições de registro e de verificação o IDSDK ficou próximo dos melhores resultados. Já o tempo de registro o IDSDK atingiu resultado pouco satisfatório, principalmente pelo fato de que essa competição foi em 2000 e a máquina da competição era um Pentium III- 450Mhz (MAIO et al., 2002a), bem inferior a máquina utilizada pelo IDSDK.

As Tabelas 4.13, 4.14 e 4.15 mostram os resultados médios dos quatro bancos de cada competição. Da mesma forma, os resultados dos competidores estão ordenados por EER e na última linha está o resultado do IDSDK. Sendo que nas Tabelas 4.14 e 4.15 são apresentados os 3 melhores resultados e os 3 piores resultados, pois houve muitos competidores nestas competições. Nos sites do FVC e no artigo de Maio (MAIO et al., 2002a), (MAIO et al., 2002b) e (MAIO et al., 2004) há uma descrição detalhada sobre os resultados.

Tabela 4.13: Resultados do médios dos bancos do FVC/2000

Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
Sag1	1.73	0.00	0.00	3.18	1.22
Sag2	2.28	0.00	0.00	1.11	0.88
Cspn	5.19	0.14	0.31	0.20	0.20
Cetp	6.32	0.00	0.02	0.95	1.06
Cwai	7.08	4.46	3.14	0.27	0.35
Krdl	10.94	6.86	6.52	1.08	1.58
Utwe	15.24	0.00	0.00	10.42	2.67
Fpin	15.94	0.00	0.00	1.22	1.27
Uinh	19.33	3.75	5.23	0.71	0.76
Diti	20.97	0.00	0.00	1.24	1.32
Ncmi	47.84	0.00	0.09	1.44	1.71
IDSDK	21.75	0.00	1.07	2.70	0.87

Pelos dados destas tabelas observa-se que o protótipo IDSDK atingiu um resultado pouco satisfatório em relação ao erro ERR, e caso participasse das competições do FVC ocuparia as últimas posições. O IDSDK também apresentou resultado fraco em relação ao Tempo de Registro (AVG_{reg}), fato que desprestigia o processo de extração de minúcias descrito na Seção 3.2.3.3. A respeito do tempo do processo de verificação pode-

Tabela 4.14: Resultados médios de todos os bancos do FVC/2002

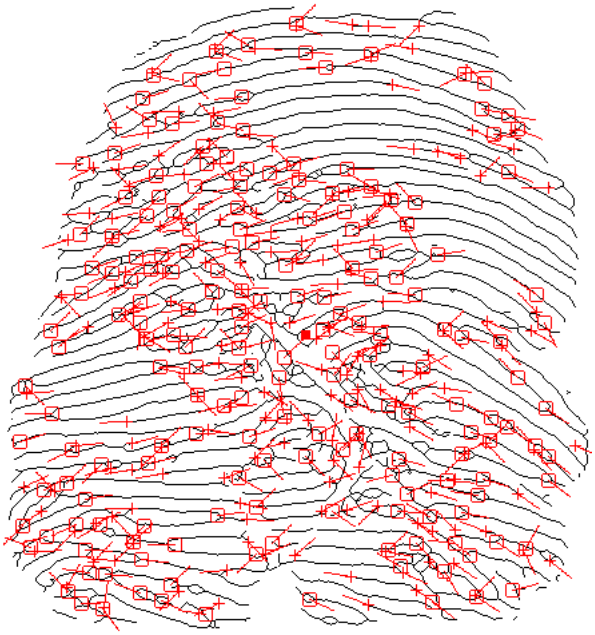
Os 3 (três) Melhores Resultados					
Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
PA15	0.19	0.00	0.00	0.11	1.97
PA27	0.33	0.00	0.00	2.12	1.98
PB15	0.41	0.00	0.00	1.23	1.13
Os 3 (três) Piores Resultados					
Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
PA16	16.79	0.00	0.53	1.16	1.19
PA25	39.10	2.50	1.81	0.52	0.63
PA03	50.00	0.0	100.00	7.05	5.01
IDSDK	23.00	0.00	0.01	3.52	1.33

Tabela 4.15: Resultados médios de todos os bancos do FVC/2004

Os 3 (três) Melhores Resultados					
Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
P101	2.07	0.00	0.00	0.08	1.48
P047	2.10	0.00	0.00	2.07	2.07
P071	2.30	0.00	0.00	0.35	0.67
Os 3 (três) Piores Resultados					
Algoritmo	EER (%)	REG_{reg} (%)	REG_{veri} (%)	AVG_{reg} (s)	AVG_{veri} (s)
P106	28.44	0.00	0.99	0.23	0.31
P079	36.77	0.00	0.00	2.07	2.80
P109	37.83	0.21	0.11	1.44	1.34
IDSDK	27.75	0.00	0.00	3.5203	0.2836

se afirmar que o método empregado pelo IDSDK possui desempenho similar aos demais competidores, sendo que o tempo de verificação varia proporcionalmente ao número de minúcias extraídas. A Figura 4.16 apresenta um exemplo de ID que consumiu bastante tempo no processo de verificação.

(a) Imagem após o filtro de Gabor



(b) As minúcias extraídas

Figura 4.16: Exemplo de uma ID que gerou um alto tempo de verificação devido ao grande número de minúcias falsas extraídas.

5 CONCLUSÕES

"Mesmo que tudo o que penso seja falso,
resta a certeza de que penso."

René Descartes, *Meditações*

5.1 Sobre a Pesquisa

O objetivo desta pesquisa foi o de estudar e avaliar diferentes técnicas empregadas no Processo de Reconhecimento de Identidade por Impressões Digitais (PRIID). Além da fundamentação teórica sobre o tema, buscou-se uma complementação prática através da construção de um protótipo (IDSDK) em Matlab para avaliar e validar os principais algoritmos estudados.

No Capítulo 2 desta dissertação faz-se uma análise sobre a necessidade da comprovação de identidade na sociedade contemporânea. Neste mesmo capítulo apresenta-se a forma de prova de identidade por biometria, acompanhado pela apresentação das características de projeto, de funcionamento e de avaliação dos Sistemas Biométricos. Também é feita uma descrição sobre as particularidades da impressão digital, tais como, sua formação, seu uso, suas classes, suas características etc.

No capítulo seguinte discorre-se sobre o PRIID em si e sobre as técnicas mais empregadas em cada uma das etapas do processo. Neste capítulo também são descritos os detalhes de implementação de algumas técnicas escolhidas para inclusão no protótipo.

No Capítulo 4 apresenta-se o critério de avaliação adotado pela competição de verificação de impressão digital (FVC), bem como os resultados do método de extração de singularidades (método de índice de Poincaré e o método proposto por Jain et al. (2002)), do método de extração de minúcias e o método de verificação (Centróide, Exaustivo, Singularidade e Características Locais). Por fim, faz-se um estudo comparativo do

desempenho alcançado pelas técnicas implementados no IDSDK como os algoritmos dos competidores do FVC de 2000, 2002 e 2004.

5.2 Sobre as Técnicas Implementadas

Neste trabalho foram implementados quatro métodos de extração de características: a extração de singularidades - método do índice de Poincaré e o método proposto por Jain et al. (2000) -, a extração clássica de minúcias e a extração de características locais.

A extração de singularidades pelo método de índice de Poincaré apresentou uma alta ocorrência de detecção de falsas singularidades ($75,30\%$ para $\Delta s = 10$ *pixels*) e uma baixa ocorrência de ausência de detecção de singularidades existentes ($5,04\%$ para $\Delta s = 30$ *pixels*). Seu desempenho foi fraco principalmente na extração da singularidade do tipo Delta. Pelos testes realizados, conclui-se que este método é bastante dependente da qualidade da imagem e que a maioria dos seus erros se situou nas regiões do contorno da imagem após aplicação do filtro de Gabor. Outro fato negativo deste método é a sua baixa precisão, como ele trabalha sobre o campo direcional, a precisão da posição da singularidade é inversamente proporcional ao tamanho da máscara utilizada na construção do campo direcional.

A extração de singularidades pelo método proposto por Jain et al. (2000) apresentou um resultado melhor que o método de Poincaré (Ver Tabela 4.2), principalmente em relação a taxa de acerto. Conta a favor deste método o fato de não precisar do aprimoramento da imagem, já o fator negativo é que ele só detecta singularidade do tipo Núcleo. Embora possua um desempenho superior ao método de Poincaré, esperava-se que este método atingisse maiores taxas de acerto. Na investigação do motivo deste fraco desempenho percebeu-se que a singularidade extraída por este método ficava realmente distante da marcação manual, porém ela também se situava numa região típica de uma singularidade. Neste momento observou-se que devido ao não conhecimento da posição exata de uma singularidade não foi possível aferir de maneira confiável os resultados obtidos pelos processos de extração de singularidades implementados.

A extração de minúcias implementada emprega a técnica mais difundida na literatura científica. Este método consiste na limiarização e no afinamento da imagem, e por fim o cálculo do *crossing number*. Pelo valor do *crossing number* determina-se a

posição e o tipo das minúcias. A fim de se eliminar minúcias espúrias e simplificar o cálculo do ângulo da minúcia, optou-se por localizar as minúcias do tipo de bifurcação através da imagem negativa. Isso fez que o processo de limiarização, afinamento e cálculo do *crossing number* fossem executados duas vezes (uma para a imagem normal e outra para a imagem negativa). Pelos resultados obtidos observou-se que esta forma gerou um grande desperdício de tempo, o que é confirmado pelos dados da Tabela 4.12 onde o tempo do IDSDK ficou acima da média mesmo utilizando máquina de melhor desempenho.

Em relação ao desempenho (acurácia) do método de extração de minúcias nada se pode afirmar, pois não é conhecida a posição, o ângulo nem o tipo correto das minúcias presentes nas ID da base de teste. Também por ser uma tarefa muito dispendiosa não foi possível marcar manualmente as posições das minúcias. Sendo assim, a extração acabou sendo medida indiretamente pelo processo de verificação.

O desempenho do processo de extração de características locais só foi medido em relação ao seu tempo de processamento. Pelos dados da Tabela 4.10 pode-se observar que ele consome um tempo razoável, mas nada que impossibilite seu emprego em um PRIID.

Também foram implementados quatro métodos de verificação: Centróide, Exaustivo, Singularidade e por Características Locais. A principal característica da ID utilizada nestes 4 (quatro) métodos foi o conjunto de minúcias. Como visto no Capítulo 3, o problema de verificação de ID baseado nas minúcias pode ser categorizado como um problema de *pattern point matching*, e a literatura científica apresenta diversas abordagens para solucionar este problema. A abordagem escolhida foi a da transformação rígida.

Desta forma, o método de verificação incluía a determinação do ângulo de rotação e o deslocamento entre as minúcias das duas ID a serem comparadas, a aplicação da transformação linear e o cálculo do grau de similaridade. A determinação do ângulo de rotação e o deslocamento foram feitos pela diferença espacial e angular entre duas minúcias consideradas como equivalentes. Os quatro métodos implementados somente se distinguem na escolha do par de minúcias a serem consideradas equivalentes.

O método do Centróide escolhe o par de minúcias equivalente entre as combinações das 3 (três) minúcias mais próximas do centro de massa de cada imagem da ID. Portanto, neste método, a escolha do par de minúcias equivalentes é altamente dependente da posição da ID na aquisição de imagem. Ou seja, para cada processo de aquisição a re-

gião central da imagem da ID coletada deve retratar sempre a mesma região da ID. Caso não retrate, a escolha do par de minúcias equivalentes será errada, e por conseqüência o método de verificação também. Nos testes sobre o banco DB1 do FVC/2000 apresentados no Apêndice B, este método alcançou um desempenho pouco satisfatório com um ERR_{medio} da ordem de $33,25\%$.

O método Exaustivo considera todos os pares de minúcias equivalentes possíveis. Como era esperado, este método consome muito mais tempo de processamento. Nos testes sobre o banco DB1 do FVC/2000 apresentados no Apêndice C, o tempo médio de verificação sempre ficou acima de 4s. Apesar deste contratempo, o método exaustivo atingiu um ERR_{medio} igual a $15,33\%$, que é um valor razoável. No entanto, este método não alcançou uma boa separação entre os histogramas genuíno e impostor nos testes realizados.

O método da Singularidade determina o par de minúcias equivalentes entre as combinações das 3 (três) minúcias mais próximas da singularidade de cada ID. Caso haja mais de uma singularidade, escolhe-se a singularidade mais próxima do centro de massa. Caso não haja singularidade, escolhe-se o centro de massa da imagem. Este método não é tão dependente do processo de aquisição quanto o método do centróide, já que a escolha do par de minúcias equivalentes é feita pela posição relativa das minúcias - mais próximas da singularidade. Contudo, é necessário se conhecer a posição e o tipo da singularidade, o que exige a extração de singularidade. O ERR_{medio} alcançado nos testes sobre o banco DB1 do FVC/2000 (ver Apêndice D) deste método foi igual a $29,25\%$, obtendo assim um resultado melhor que o método do Centróide.

O método por Características Locais determina o par de minúcias equivalentes a partir de 3 (três) pares de minúcias com maior grau de similaridade entre seus respectivos vetores de características locais. Por trabalhar em cima das características locais este é método mais robusto, pois dificilmente escolherá uma minúcia espúria como uma minúcia equivalente. Também é mais resistente a deformação não linear da ID gerada no processo de aquisição. Nos testes executados sobre o banco DB1 do FVC/2000 (ver Apêndice E), o método por Características Locais apresentou um ERR_{medio} igual a $23,25\%$. Apesar de ser um valor maior que o atingindo pelo método exaustivo, o método por Características Locais foi considerado o melhor método de verificação implementado em razão do seu baixo tempo de processamento e pela separação alcançada entre a distribuição genuíno e

impostor.

Sendo assim, o método de verificação por Características Locais - com os parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30^{o}$ - foi aplicado sobre as demais bases de teste (Ver Apêndice F). Os resultados obtidos foram comparados com os resultados das competições do FVC de 2000, 2002 e 2004 (Ver Tabelas 4.13, 4.14 e 4.15). A princípio, sobre esses resultados chega-se a duas possíveis conclusões: o método de verificação por características locais por si só é um método ineficiente ou o método de extração de características (extração de minúcias, singularidade e características locais) possui desempenho ruim e propaga seus erros para a etapa de verificação. Entretanto, este resultado pouco satisfatório não desmerece as técnicas implementadas nesta pesquisa. A base de teste das competições do FVC foi exatamente construída de forma a explorar as grandes dificuldades inerentes ao PRIID. As técnicas implementadas são os primeiros passos da construção de um sistema eficiente.

Conclui-se, então, que a grande dificuldade a ser superada no PRIID, diz respeito à má qualidade da imagem e da própria ID, aos ruídos inerentes ao processo e à translação, rotação, sobreposição parcial e distorção não linear geradas no processo de aquisição. Desta forma, um PRIID robusto e eficiente constitui-se de um aglomerado de técnicas e métodos que atacam todas essas dificuldades.

5.3 Dificuldades Encontradas

A idéia inicial desta pesquisa era propor uma nova abordagem para o problema da verificação de ID que fosse baseado em técnicas de inteligência computacional. Porém, seria necessário ter em mãos um conjunto de características de ID já extraídas de uma base de teste conhecida. A superação desta dificuldade veio com a utilização da base de teste da competição do FVC disponibilizadas no livro de Maltoni et al. (2003) e com a construção dos próprios dados relativos a essas imagens a partir da implementação das técnicas mais difundidas, o que no final se tornou o principal objetivo da pesquisa.

Outra curiosa dificuldade encontrada foi o grande número de trabalhos publicados sobre o assunto, que no primeiro momento não seria dificuldade, porém alguns trabalhos apresentam conclusões conflitantes o que gerou uma incerteza quanto o desempenho esperado de certos métodos. Por fim, o fato de se trabalhar sobre 10560 imagens consumiu muito tempo na consolidação dos resultados.

5.4 Contribuições

A principal contribuição deste trabalho foi a construção de um protótipo de um Sistema de Verificação de Identidade por Impressões Digitais. Este protótipo contém as principais técnicas implementadas e também serve como ferramenta de visualização das operações sobre a imagem da ID e das características extraídas. Outro contribuição desta pesquisa são os dados produzidos (características da ID) e os resultados obtidos. Estas contribuições poderão atuar como uma plataforma para futuros trabalhos de pesquisa.

5.5 Trabalhos Futuros

Partindo do que foi feito neste trabalho, sugere-se como possíveis estudos futuros a abordagem dos seguintes temas:

- Produzir uma base de dados com as marcações manuais de minúcias para possibilitar uma avaliação e aprimoramento de algoritmos de extração de minúcias;
- Melhorar a base de dados com as marcações manuais de singularidades para possibilitar uma avaliação e aprimoramento de algoritmos de extração de singularidades;
- Melhor o algoritmo de aprimoramento da imagem baseado no filtro de Gabor proposto por Marques (2004);
- Melhorar o método de detecção e eliminação de minúcias espúrias;
- Conceber um método de extração de minúcias a partir de uma imagem em tons de cinza, sem a necessidade do afinamento da imagem;
- Conceber um método mais eficiente e robusto para a determinação de minúcias equivalentes e justaposição das ID;
- Conceber e testar outras formas de cálculo do grau de similaridade entre dois conjuntos de minúcias;

REFERÊNCIAS

BARBOZA, J. L. L. **Processamento de Imagens Aplicado à Monitoração de Processos.** Rio de Janeiro, 2005. Dissertação (Mestrado em Informática) - Universidade Federal do Rio de Janeiro, 2005. Disponível em: <https://www.labic.nce.ufrj.br>. Acesso em: 03 mar. 2005.

BAZEN, A. M.; GEREZ S. H. Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 24, n. 7, p. 905-919, jul. 2002.

BURGE, M.; BURGER, W. Ear Biometrics in Computer Vision . **15th International Conference on Pattern Recognition**, v. 2, p.822-826, set. 2000.

CAPPELLI, R; LUMINI, A. Fingerprint Classification by Directional Image Partitioning. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 21, n. 5, p. 402-421, mai. 1999.

CAPPELLI, R; MAIO, D; MALOTNI, D; WAYMAN, J. L.; JAIN, A. K. Performance Evaluation of Fingerprint Verification Systems. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 28, n. 1, p. 3-18, jan. 2006. Disponível em: <http://biometrics.cse.msu.edu/publications.html>. Acesso em: 28 jun. 2006.

CHIKKERUR, S. S. **Online Fingerprint Verification System.** Buffalo, 2005. Dissertação (Mestrado em Engenharia Elétrica) - State University of New York at Buffalo, 2005. Disponível em: <web.mit.edu/ sharat/www/research/thesis.pdf>. Acesso em: 17 fev. 2006.

COSTA, S. M. F. **Classificação e Verificação de Impressões Digitais.** São Paulo, 2001. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de São Paulo, 2001. Disponível em: <http://www.teses.usp.br>. Acesso em: 03 fev. 2005.

DAGHER, I.; HELWE, W.; YASSINE, F. Fingerprint Recognition using Fuzzy Artmap

Neural Network Architecture. **The 14th International Conference on Microelectronics 2002**, p. 157-160, dez. 2002.

DUTA, N.; JAIN, A. K.; MARDIA, K. V. Matching of Palmprints. **Pattern Recognition Letters**, p. 477-485, v. 23, n.4, abr. 2002.

ERN, L.C.; SULONG, G. Fingerprint Classification Approaches: an Overview. **Sixth International Symposium on Signal Processing and its Applications**, Kuala Lumpur, v. 1, p. 347-350, ago. 2001.

FARINA, A.; KOVACS-VAJNA, Z. M. Fingerprint Minutiae Extraction from Skeletonized Binary Images. **Pattern Recognition**, v. 32, n. 5, p. 877-889, mai. 1999.

FOGAÇA, C. RG Funerário. **Revista Superinteressante**. São Paulo: Editora Abril, ed. 183, p. 37, dez. 2002.

GAO, Q.; MOSCYTZ, G. S. Fingerprint Feature Matching using CNNs. **Proceedings of the International Symposium on Circuits and Systems, 2004. ISCAS '04**, v. 3, p. 73-76, mai. 2004.

GERMAIN, R. S.; CALIFANO, A.; COLVILLE, S. Fingerprint Matching using Transformation Parameter Clustering. **IEEE Computational Science and Engineering**, v. 4, n. 4, p. 42-49, out./dez. 1997.

GONZALEZ, R. C.; WOODS, R. E. **Processamento de Imagens Digitais.** São Paulo: Editora Edgard Blücher LTDA, 2000.

GUO, H.; OU, Z. Y.; HE, Y. Automatic Fingerprint Classification Based on Embedded Hidden Markov Models. **Proceedings of the Second International Conference on Machine Learning and Cybernetics**, Xian, p. 3033-3038, nov. 2003.

HALICI, U.; ONGUN, G. Fingerprint Classification through Self-organizing Feature Maps Modified to Treat Uncertainties. **Proceedings of the IEEE**, v. 84, n. 10, p. 1497-1512, out. 1996.

HAO, Y.; TAN, T.; WANG, Y. Fingerprint Matching based on Error Propagation. **Proceedings of International Conference on Imagem Processing**, p. 273-276, 2002.

HONG, L. **Automatic Personal Identification Using Fingerprints.** East Lansing, 1998. Tese (Doutorado em Ciência da Computação) - Michigan State University, 1998.

Disponível em: <http://biometrics.cse.msu.edu/publications.html>. Acesso em: 26 abr. 2005.

HONG, L.; JAIN, A. K.; PANKANTI, S.; BOLLE, R. Fingerprint Enhancement. **3rd IEEE Workshop on Applications of Computer Vision (WACV '96)**, Sarasota, p. 202-207, dez. 1996.

HSIEH, C. T.; LU, Z. Y.; LI, T.C; MEI, K. C. An Effective Method to Extract Fingerprint Singular Point. **The Fourth International Conference on High-Performance Computing in the Asia-Pacific Region**, v. 2, p. 696, jan. 2000

HUVANANDANA, S.; MALISUWAN, S.; SANTIYANON, J.; HWANG, J. A Hybrid System for Automatic Fingerprint Identification. **Proceedings of the 2003 International Symposium on Circuits and Systems**, v. 2, p. 952-955, mai. 2003

JAIN, A. K. **Fundamentals of Digital Image Processing.** New York: Prentice-Hall, 1988.

JAIN, A. K.; HONG, L. On-line Fingerprint Verification. **Proceedings of the 13th International Conference on Pattern Recognition**, v. 3, p. 25-29, ago. 1996.

JAIN, A. K.; PANKANTI, S.; PRABHAKAR, S.; HONG, L.; ROSS, A.; WAYMAN, L. J. Biometrics: a Grand Challenge. **Proceedings of International Conference on Pattern Recognition (ICPR)**, Cambridge, v. 2, p. 935-942, ago. 2004. Disponível em: <http://biometrics.cse.msu.edu/publications.html>. Acesso em: 19 mar. 2005.

JAIN, A. K.; PRABHAKAR, S.; HONG, L. A Mutichannel Approch to Fingerprint Classification. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 21, n. 4, p. 348-359, abr. 1999.

JAIN, A. K.; PRABHAKAR, S.; HONG, L.; PANKANTI, S. Filterbank-Based Fingerprint Matching. **IEEE Transactions on Image Processing**, v. 9, n. 5, p. 846-859, mai. 2000.

JAIN, A. K.; PRABHAKAR, S.; PANKANTI, S. On The Similarity of Identical Twin Fingerprints. **Pattern Recognition**, v. 35, n. 11, p. 2653-2663, nov. 2002.

JAIN, A. K.; ROSS, A. Fingerprint Mosaicking **Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)**, Orlando, Florida, v.4, p. 4064-4067, mai. 2002.

JAIN, A. K.; ROSS, A.; PANKANTI, S. A Prototype Hand Geometry-based Verification System. **2nd International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)**, Washington, p. 22-24, mar. 2004.

JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. **IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics**, v. 14, n. 1, p. 4-20, jan. 2004. Disponível em: <http://www.csee.wvu.edu/ ross/publications.shtml>. Acesso em: 19 mar. 2005.

JIA, C.; XIE, M; LI, Q. A fingerprint minutiae matching approach based on vector triangle method and ridge structure **International Conference on Communications, Circuits and Systems**, v. 2, p. 871-875, jun. 2004.

JIANG, X.; YAU, W. Fingerprint Minutiae Matching Based on the Local and Global Structures. **Proceendings 15th International Conference on Pattern Recognition**, v. 2, p. 1042-1045, jan. 2000.

JIANG, X.; LIU, M.; KOT, A. C. Reference Point Detection for Fingerprint Recognition. **Proceendings 17th International Conference on Pattern Recognition**, v. 1, p. 540-543, jan. 2000.

JIN, A. L. H; CHEKIMA, A.; DARGHAM, J.A.; LIAU, C. F. Fingerprint identification and recognition using backpropagation neural network. **Student Conference on Research and Development, 2002. SCOReD 2002**, Shah Alam, p. 98-101, jul. 2002.

KAZIENKO, J. F. **Assinatura digital de documentos eletrônicos através da impressão digital.** Florianópolis, 2003. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Santa Catarina, 2003. Disponível em: <https://www.labsec.ufsc.br>. Acesso em: 10 mar. 2005.

KO, T. Fingerprint Enhancement by Spectral Analysis Techniques. **Proceedings of the 31st Applied Imagery Pattern Recognition Workshop**, Washington, p. 133-139, out . 2002.

KOVACS-VAJNA, Z. M. A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 22, n. 11, p. 1266-1276, nov. 2000.

LAM, L.; LEE, S. W.; Suen, C. Y. Thinning Methodologies-A Comprehensive Survey . **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 14, n.9, p.869-885, set. 1992.

LE, T. V.; CHEUNG, K. Y.; NGUYEN, M. H. A Fingerprint Recognizer using Fuzzy Evolutionary Programming. **Proceedings of the 34th Annual Hawaii International Conference on System Sciences**, p. 7, jan. 2001.

LEE, S. W.; NAM, B. H. Fingerprint Recognition using Wavelet Transform and Probabilistic Neural Network. **International Joint Conference on Neural Networks, IJCNN '99**, v. 5, p. 3276-3279, jul. 1999.

LEE, C. J.; WANG, S. D. A Gabor filter-based approach to fingerprint recognition. **IEEE Workshop on Signal Processing Systems**, Taipei, p. 371-378, 1999.

LI, B.; MENG, Q; HOLSTEIN, H. Point Pattern Matching and Applications-a review. **IEEE International Conference on Systems, Man and Cybernetics**, v. 1, p. 729-736, out. 2003.

LIMA, A. R. G. **Máquinas de Vetores Suporte na Classificação de Impressões Digitais.** Fortaleza, 2002. Dissertação (Mestrado em Computação) - Universidade Federal do Ceará, 2002. Disponível em: <http://www.mcc.ufc.br/disser/AllanReffson.pdf>. Acesso em: 03 fev. 2006.

LOBATO, E.; SEARA, R. Classificação e Identificação de Impressões Digitais em Tempo Real através de Análise de Multi-Resolução da Informação Direcional. **XVIII Simpósio Brasileiro de Telecomunicações**, set. 2000.

LU, X.; COLBRY, D.; JAIN, A. K. Three-Dimensional Model Based Face Recognition. **Proceedings of International Conference on Pattern Recognition (ICPR)**, Cambridge, v. 1, p. 362-366, ago. 2004.

LU, X.; HSU, R.; JAIN, A. K.; KAMGAR-PARSI, B. Face Recognition with 3D Model-Based Synthesis. **Proceedings International Conference on Biometric Authentication (ICBA)**, p. 139-146, jul. 2004.

LUO, X.; TIAN, J.; WU, Y.. A Minutia Matching Algorithm in Fingerprint Verification. **15th International Conference on Pattern Recognition**, v. 4, p. 4833, jan. 2000.

MAIO, D.; MALOTNI, D. A Structural Approach to Fingerprint Classification. **13th International Conference on Pattern Recognition (ICPR'96)**, Viena, v. 3, n. 3, p. 578, ago. 1996.

MAIO, D; MALOTNI, D; CAPPELLI, R.; WAYMAN, J. L.; JAIN, A. K. FVC2000: Fingerprint Verification Competition. **IEEE Transactions on Pattern Analysis and**

Machine Intelligence, v. 24, n. 3, p. 402 - 412, mar. 2002. Disponível em: <http://biometrics.cse.msu.edu/publications.html>.Acesso em: 28 abr. 2005.

MAIO, D; MALOTNI, D; CAPPELLI, R.; WAYMAN, J. L.; JAIN, A. K. FVC2002: Fingerprint Verification Competition. **Proceedings of International Conference on Pattern Recognition**, Quebec City, p. 811-814, ago. 2002. Disponível em: <http://biometrics.cse.msu.edu/publications.html>.Acesso em: 28 abr. 2005.

MAIO, D; MALOTNI, D; CAPPELLI, R.; WAYMAN, J. L.; JAIN, A. K. FVC2004: Fingerprint Verification Competition. **Proceedings of International Conference on Biometric Authentication (ICBA)**, Hong Kong, p. 1-7, jul 2004. Disponível em: <http://biometrics.cse.msu.edu/publications.html>.Acesso em: 28 abr. 2005.

MALTONI, D.; MAIO, D; JAIN, A. K.; PRABHAKAR, S. **Handbook of Fingerprint Recognition.** New York: Springer, 2003.

MARQUES, A. C. P. B. **Extração de minúcias em imagens de impressões digitais utilizando redes neurais.** Rio de Janeiro, 2004. Dissertação (Mestrado em Informática) - Universidade Federal do Rio de Janeiro, 2004. Disponível em: <https://www.labic.nce.ufrj.br>. Acesso em: 03 fev. 2005.

MARQUES, A. C. P.B.; THOMÉ, A. C. G. A Neural Network Fingerprint Segmentation Method. **Fifth International Conference on Hybrid Intelligent Systems**, v. 1, p. 385-392, nov. 2005.

MOHAMED, S.M.; NYONGESA, H. Automatic Fingerprint Classification System using Fuzzy Neural Techniques. **FUZZ-IEEE'02. Proceedings of the 2002 IEEE International Conference on Fuzzy Systems**, v.1, p. 358-362, mai. 2002.

MOON, Y.S.; YEUNG, H.W.; CHAN, K.C.; CHAN, S.O. **IEEE International Proceedings Acoustics, Speech and Sinal Processing (ICASSP' 04)**, v.5, p. 409-412, mai. 2004.

MOUTINHO, A. M. **Identificação de Padrões Faciais Usando Redes Neurais Artificiais.** Rio de Janeiro, 2005. Dissertação (Mestrado em Informática) - Universidade Federal do Rio de Janeiro, 2005.

NAGATY, K. A. An energy-based fingerprint matching system. **First IEEE Consumer Communications and Networking Conference**, p. 706-709, jan. 2004.

NETO, H. V.; BORGES, D. L. Fingerprint Classification with Neural Networks. **4th Brazilian Symposium on Neural Networks (SBRN '97)**, Goiânia, p. 66, dez. 1997.

O'GORMAN, L. Comparing Passwords, Tokens, and Biometrics for User Authentication **Proceedings of the IEEE**, v. 91, n. 12, p. 2019-2040, dez. 2003. Disponível em: <http://www.research.avayalabs.com/user/logorman/>. Acesso em: 26 abr. 2005.

O'GORMAN, L. Seven issues with human authentication technologies. **Proceedings of Workshop on Automatic Identification Advanced Technologies - (AutoID)**, Tarrytown, p. 185-186, mar. 2002. Disponível em: <http://www.research.avayalabs.com/user/logorman/>. Acesso em: 26 abr. 2005

OLIVEIRA, M. A.; LEITE, N. J. Reconnection of Fingerprint Ridges Based on Morphological Operators and Multiscale Directional Information. **XVII Simpósio Brasileiro de Computação Gráfica e Processamento de Imagens**, Curitiba, out. 2004.

PANKANTI, S.; PRABHAKAR, S.; JAIN, A. K. On the Individuality of Fingerprints. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 24, n. 8, p. 1010-1025, ago. 2002. Disponível em: <http://www.csee.wvu.edu/ ross/publications.shtml>. Acesso em: 28 jun. 2006.

PRABHAKAR, S. **Fingerprint Classification and Matching Using a Filterbank.** East Lansing, 2001. Tese (Doutorado em Engenharia) - Michigan State University, 2001. Disponível em: <http://www.csee.wvu.edu/ ross/publications.shtml>. Acesso em: 19 mar. 2005.

ROSS, A. **Information Fusion in Fingerprint Authentication.** East Lansing, 2003. Tese (Doutorado em Engenharia) - Michigan State University, 2003. Disponível em: <http://www.csee.wvu.edu/ ross/publications.shtml>. Acesso em: 19 mar. 2005.

ROSS, A.; JAIN A. K. Multimodal Biometrics: An Overview.**Proceedings of 12th European Signal Processing Conference (EUSIPCO)**, Viena, p.1221-1224, set. 2004.

ROSS, A.; JAIN A. K.; REISMAN, J. A Hybrid fingerprint matcher. **Pattern Recognition**, v. 36, n. 7, p.1661-1673, jan. 2003.

SALEH, A. A.; ADHAMI R. R. Curvature-based Matching Approach for Automatic Fingerprint Identification. **Proceedings of the 33rd Southeastern Symposium on System Theory**, Athens, p. 171-175, mar. 2001.

SELVARAJ, H.; ARIVAZHAGAN S.; GANESAN, L. Fingerprint Verification Using Wavelet Transform . **Proceedings of the 5th International Conference on Computational Intelligence and Multimedia Applications**, Washington, p. 430, 2003.

SHA, L.; TANG X. Orientation-improved Minutiae for Fingerprint Matching. **Proceedings of the 17th International Conference on Pattern Recognition**, v. 4, p. 432-435, ago. 2004.

SHAH, S.; SASTRY P. S. Fingerprint Verification Using Wavelet Transform. **IEEE Transactions on Systems, Man and Cybernetics**, v. 34, n. 1, p. 84-94, fev. 2004.

SUCUPIRA, L. H. R. J. **Uma Metodologia para Avaliação de Pacotes de Software Biométricos.** Campinas, 2004. Dissertação (Mestrado em Engenharia Elétrica e de Computação) - Universidade Estadual de Campinas, 2004. Disponível em: <http://libdigi.unicamp.br>. Acesso em: 03 fev. 2005.

TAN, X.; BHANU, B. Fingerprint Verification using Genetic Algorithms. **Proceedings Sixth IEEE Workshop on Applications of Computer Vision (WACV 2002)**, p. 79-83, dez. 2002.

TAN, X.; BHANU, B. On the Fundamental Performance for Fingerprint Matching. **IEEE Computer Society Conference on Computer Vision and Pattern Recognition**, v. 2, p. 499-504, jun. 2003.

TAN, X.; BHANU, B.; LIN Y. Fingerprint Identification: Classification vs. Indexing **Proceedings IEEE Conference on Advanced Video and Signal Based Surveillance**, p. 151-156, jul. 2003.

TICO, M.; KUOSMANEN, P. Fingerprint matching using an orientation-based minutia descriptor. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 25, n. 8, p. 1009-1014, ago. 2003.

TONG, X. F.; TANG, X. L.; HUANG, J. H.; LI, X. Fingerprint minutiae matching based on complex minutiae vector **Proceedings of 2004 International Conference on Machine Learning and Cybernetics**, v. 6, p. 3731-3735, ago. 2004.

ULUDAG, U.; JAIN, A. K. Attacks on Biometric Systems: A Case Study in Fingerprints **Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI**, San Jose, p. 622-633, jan. 2004. Disponível em: <http://biometrics.cse.msu.edu/publications.html>. Acesso em: 26 abr. 2005.

ULUDAG, U.; ROSS, A.; JAIN, A. K. Biometric Template Selection and Update: A Case Study in Fingerprints. **Pattern Recognition**, v. 37, n. 7, p. 1533-1542, jul. 2004. Disponível em: <http://biometrics.cse.msu.edu/publications.html>. Acesso em: 28 jun. 2006.

WANG, S.; ZHANG, W. W.; WANG, Y. S. Fingerprint Classification by Directional Fields **Proceedings of Fourth IEEE International Conference on Multimodal Interfaces**, Pittsburgh, p. 395-399, out. 2002.

WAYMAN, J.; JAIN, A. K.; MALTONI, D.; MAIO, D. **Biometric Systems Technology, Design and Performance Evaluation.** New York: Springer, 2005

YAGER, N.; AMIN, A. Fingerprint Classification: a Review. **Pattern Analysis & Applications** , v. 7, n. 1, p. 77-93, abr. 2004.

YAGER, N.; AMIN, A. Fingerprint Verification based on Minutiae Features: a Review. **Pattern Analysis & Applications** , v. 7, n. 1, p. 94-113, abr. 2004.

ZHANG, W.; WANG, Y. Core-Based Structure Matching Algorithm of Fingerprint Verification. **International Conference on Pattern Recognition**, v. 16, n. 1, p. 70-74, jan. 2002.

GLOSSÁRIO

Ápice - Ver Núcleo.

Aquisição - Etapa do Sistema Biométrico responsável pela aquisição do dado biométrico.

Autenticação - É o processo de reconhecimento de identidade onde há voluntariedade do indivíduo a ser identificado. É dividida em dois tipos: a Verificação e a Identificação.

Biometria - O uso de características fisiológicas e comportamentais para reconhecer a identidade de uma pessoa.

Biométrica - O mesmo que Biometria.

Campo Direcional - É uma forma de representar um impressão digital. O mapa direcional divide a imagem da ID em é extrai a inclinação predominante nesta regiões.

Classificação - É uma etapa do processo de reconhecimento por Impressão Digital responsável pela a classificação da ID.

Core - Ver Núcleo.

Decisão - Etapa do Sistsma Biométrico responsável pela definição dos parâmetros que determinam o reconhecimento positivo ou negativo.

Delta - É um tipo de ponto singular que consiste na junção de linhas da impressão digital.

ERR - Denota a taxa de erro onde o limiar (l) é tal que $FAR(l) = FRR(l)$.

Falsa Aceitação - O mesmo que Falso Positivo.

Falsa Rejeição - O mesmo que Falso Negativo.

Falso Negativo - É uma possível resposta indesejada de um sistema biométrico, no caso, SB reconhece um usuário legítimo (Genuíno) como um usuário impostor.

Falso Positivo - É uma possível resposta indesejada de um sistema biométrico, no caso, SB reconhece um usuário impostor como um usuário legítimo (Genuíno).

Identificação - É o processo de reconhecimento de identidade onde há voluntariadade do indivíduo a ser identificado, sem no entanto informar previamente a sua identidade. É uma comparação 1:N, pode ser vista como n Verificações onde é o número de registros.

Impressão Digital Latente - São os vestígios de impressões digitais deixados em determinadas superfícies. Normalmente, são coletadas por peritos criminais em locais onde ocorreu um crime.

Indexação - É uma etapa do processo de reconhecimento por Impressão Digital que é responsável na indexação da ID afim de diminuir o espaço de busca.

Investigação - É o processo de reconhecimento de identidade onde não há voluntariedade e nem conhecimento sobre da identidade do indivíduo. Geralmente, este processo coleta ID latentes.

Matching - Termo da língua inglesa sem tradução equivalente na língua portuguesa. É o processo de comparação entre a ID de entrada e a ID de referência com o a finalidade de se deterninar se elas representam a mesma ID.

Mapa Direcional - O mesmo que Campo Direcional.

Minúcia - É uma descontinuidade presente em uma linha da ID, isto é, é uma interrupção existente no caminho de uma linha. A terminação e a bifurcação são os dois principais tipos de minúcias. Uma minúcia é representada por quatro infomações: $(x, y, \theta, tipo)$.

Núcleo - É um tipo de ponto sigular (singularidade), podendo ser subdividido em ápice (loop) e espiral (whorl).

Ponto Singular - É uma característica presente em quase todas impressões digitais. Pode ser do tipo Delta e do tipo Núcleo.

Reconhecimento - Termo genérico e amplo que significa o ato de reconhecer a identidade de um indivíduo, sem no entanto discriminar se há voluntariedade ou involuntariedade do indivíduo ou se há conhecimento prévio ou não da identidade do indivíduo em questão.

Reconhecimento Genuíno - É o processo de confrontar duas representações distintas de uma mesma ID. Avalia o Taxa de Falsa Rejeição de um processo de reconhecimento.

Reconhecimento Impostor - É o processo de confrontar duas representações de diferentes ID. Avalia o Taxa de Falsa Aceitação de um processo de reconhecimento.

Representação - Etapa do Sistema Biométrico responsável pela construção da representação do dado biométrico.

Singularidade - Ver Ponto Singular.

Verificação - É o processo de reconhecimento de identidade onde há voluntariadade do indivíduo a ser identificado e é informado previamente a identidade. É uma comparação 1:1.

ZeroFAR - É a menor Taxa de Falsa Rejeição (FRR) tal que não ocorra Falsa Aceitação.

ZeroFRR - É a menor Taxa de Falsa Aceitação (FAR) tal que não ocorra Falsa Rejeição.

APÊNDICE A - RESULTADOS - EXTRAÇÃO DE CARACTERÍSTICAS

Este apêndice apresenta as estatísticas sobre o tempo consumido na extração de minúcias e na extração de características locais de todas as bases de dados do FVC de 2000, 2002 e 2004.

Tabela A.1: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB1/FVC2000

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	1.8000	0.4130
Mediana	1.7800	0.4060
Mínimo	1.5500	0.1090
Máximo	2.7500	1.0780
Desvio Padrão	0.1200	0.1140

Tabela A.2: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB2/FVC2000

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	1.799	0.2081
Mediana	1.7500	0.2030
Mínimo	1.2970	0.0000
Máximo	2.9530	0.5780
Desvio Padrão	0.1874	0.0678

Tabela A.3: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB3/FVC2000

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	4.1822	0.6264
Mediana	4.0470	0.5310
Mínimo	3.3130	0.1720
Máximo	7.6870	2.5930
Desvio Padrão	0.5404	0.3448

Tabela A.4: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB4/FVC2000

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	1.4655	0.2285
Mediana	1.4530	0.2180
Mínimo	1.2660	0.0940
Máximo	2.1560	0.7030
Desvio Padrão	0.0975	0.0700

Tabela A.5: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB1/FVC2002

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	2.7430	0.2927
Mediana	2.7190	0.2820
Mínimo	2.2970	0.0930
Máximo	4.5470	0.6250
Desvio Padrão	0.2281	0.0794

Tabela A.6: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB2/FVC2002

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	3.3683	0.4147
Mediana	3.1560	0.3910
Mínimo	2.7500	0.1410
Máximo	5.6720	1.1560
Desvio Padrão	0.5255	0.1347

Tabela A.7: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB3/FVC2002

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	4.3168	0.6220
Mediana	4.1090	0.5310
Mínimo	3.3280	0.1560
Máximo	7.7500	2.5160
Desvio Padrão	0.6963	0.3439

Tabela A.8: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB4/FVC2002

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	2.0549	0.2615
Mediana	2.0150	0.2500
Mínimo	1.7500	0.0940
Máximo	3.6410	0.5940
Desvio Padrão	0.2154	0.0796

Tabela A.9: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB1/FVC2004

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	5.5107	0.4491
Mediana	5.4530	0.4220
Mínimo	4.6410	0.1410
Máximo	8.2970	1.2970
Desvio Padrão	0.4167	0.1465

Tabela A.10: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB2/FVC2004

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	2.2039	0.2438
Mediana	1.8590	0.2340
Mínimo	1.8590	0.0470
Máximo	3.0940	0.7810
Desvio Padrão	0.1813	0.0886

Tabela A.11: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB3/FVC2004

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	2.8744	0.4243
Mediana	2.7970	0.4060
Mínimo	1.9690	0.0150
Máximo	5.3440	1.1250
Desvio Padrão	0.3016	0.1335

Tabela A.12: Estatísticas sobre o Tempo Consumido na Extração de Minúcias e na Extração de Características Locais - Base de Imagens DB4/FVC2004

	Extração de Minúcias (s)	Extração de Características Locais (s)
Média	2.0700	0.3053
Mediana	2.0620	0.2970
Mínimo	1.7820	0.0940
Máximo	2.6870	0.7810
Desvio Padrão	0.1200	0.0937

APÊNDICE B - RESULTADOS - MÉTODO DO CENTRÓIDE

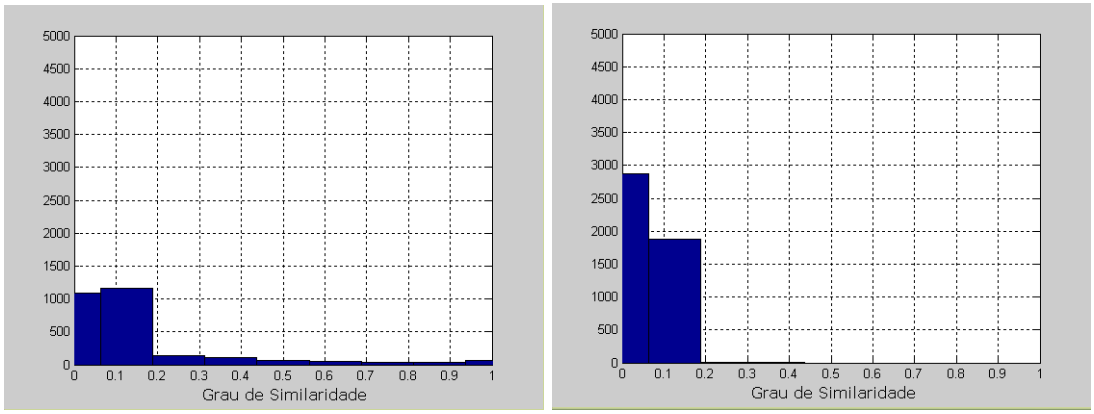
Este apêndice apresenta as estatísticas e os resultados obtidos pelo processo de verificação utilizando o método do centróide aplicado sobre o banco DB1 do FVC de 2000.

Tabela B.1: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_CENTROIDE_1A

TESTE_CENTROIDE_1A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.14	2.91	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	31.00	0.06s
Desvio Padrão	0.22	3.21	0.01s
	Reconhecimento Impostor		
Média	0.04	1.48	0.03s
Mediana	0.00	1.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	0.33	5.00	0.06s
Desvio Padrão	0.04	0.55	0.01s
$REJ_{veri} = 0.00$	$EER = 0.40$	$ZeroFAR = 0.89$	$ZeroFRR = 1.00$

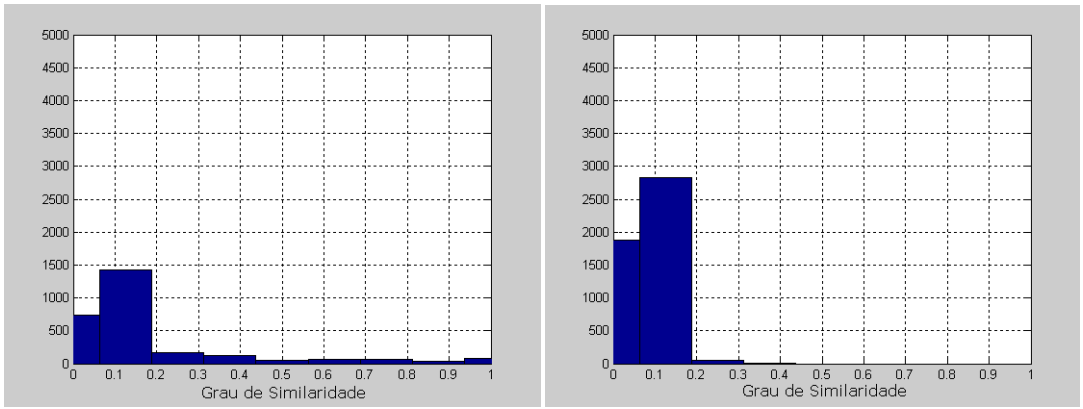
Tabela B.2: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_CENTROIDE_2A

TESTE_CENTROIDE_2A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.17	3.28	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	29.00	0.09s
Desvio Padrão	0.23	3.40	0.01s
	Reconhecimento Impostor		
Média	0.06	1.78	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	0.33	5.00	0.08s
Desvio Padrão	0.05	0.66	0.01s
$REJ_{veri} = 0.00$	$EER = 0.37$	$ZeroFAR = 0.87$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.1: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_1A



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.2: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_2A

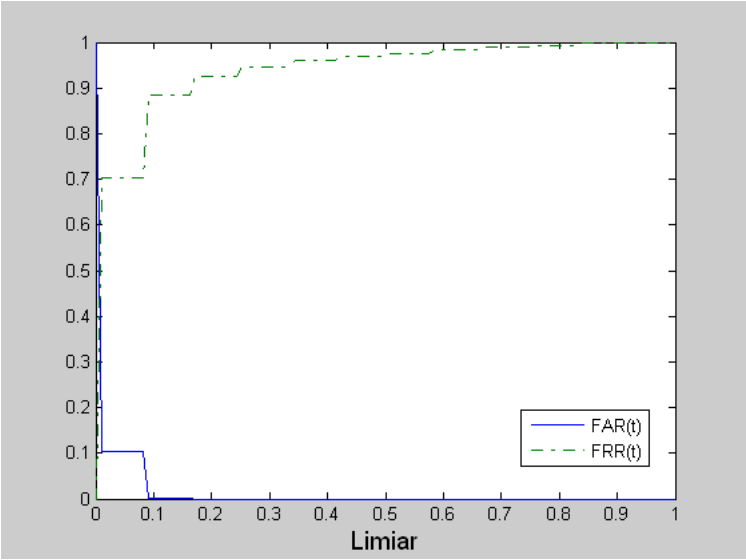


Figura B.3: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_1A

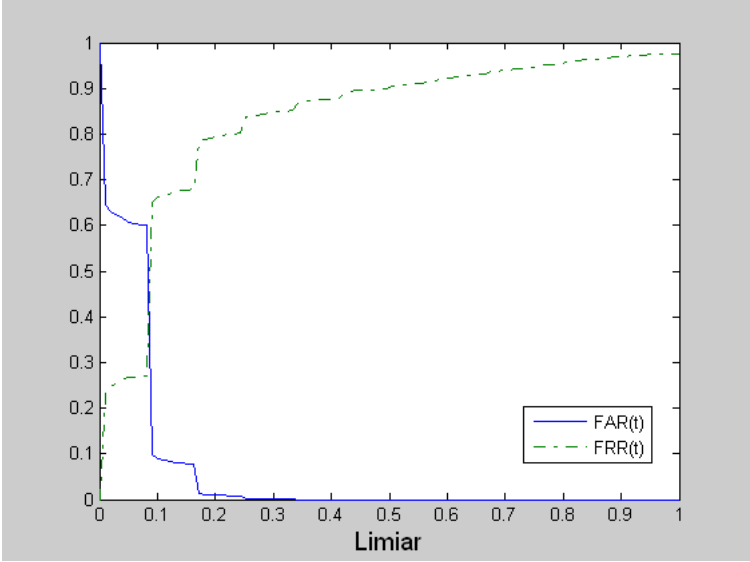


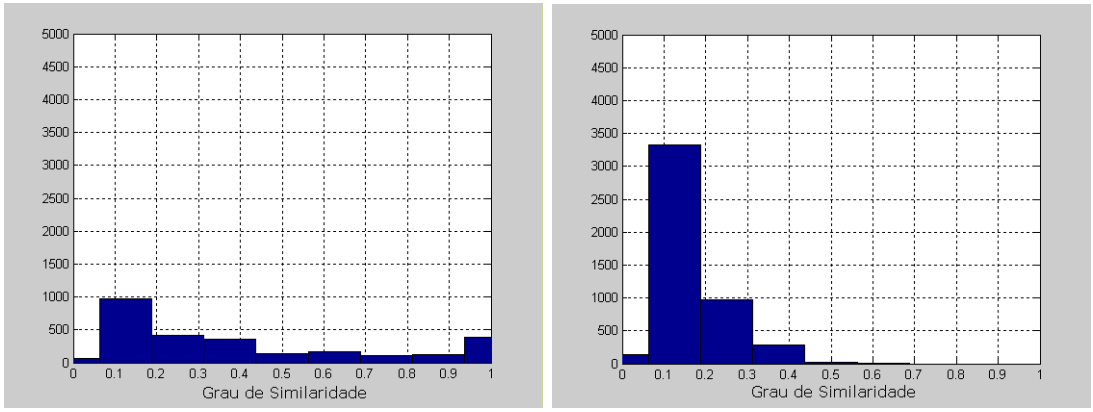
Figura B.4: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_2A

Tabela B.3: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_CENTROIDE_1B

TESTE_CENTROIDE_1B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.41	6.62	0.03s
Mediana	0.25	4.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	33.00	0.06s
Desvio Padrão	0.32	5.23	0.01s
	Reconhecimento Impostor		
Média	0.16	3.07	0.03s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	0.67	9.00	0.06s
Desvio Padrão	0.08	1.06	0.01s
$REJ_{veri} = 0.00$	$EER = 0.32$	$ZeroFAR = 0.77$	$ZeroFRR = 1.00$

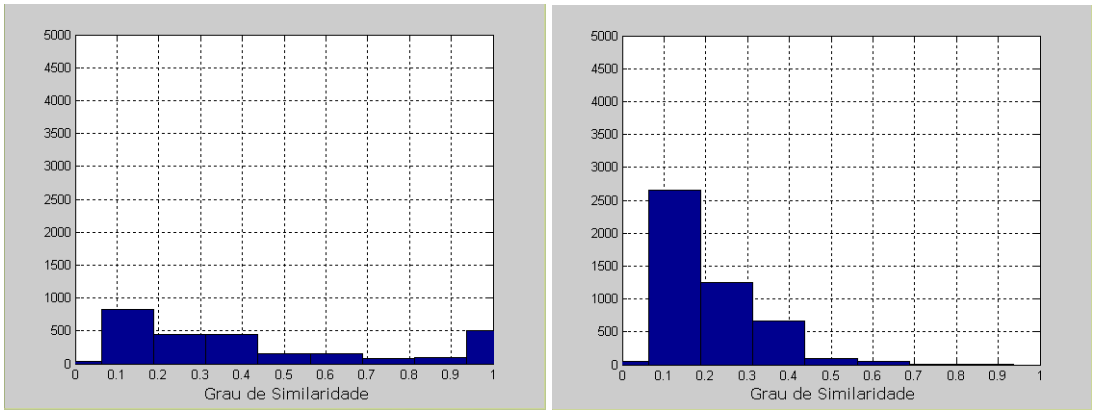
Tabela B.4: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_CENTROIDE_2B

TESTE_CENTROIDE_2B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.44	7.60	0.03s
Mediana	0.33	5.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	44.00	0.08s
Desvio Padrão	0.33	6.37	0.01s
	Reconhecimento Impostor		
Média	0.21	3.62	0.03s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.92	12.00	0.08s
Desvio Padrão	0.11	1.36	0.01s
$REJ_{veri} = 0.00$	$EER = 0.33$	$ZeroFAR = 0.81$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.5: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_1B



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.6: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_2B

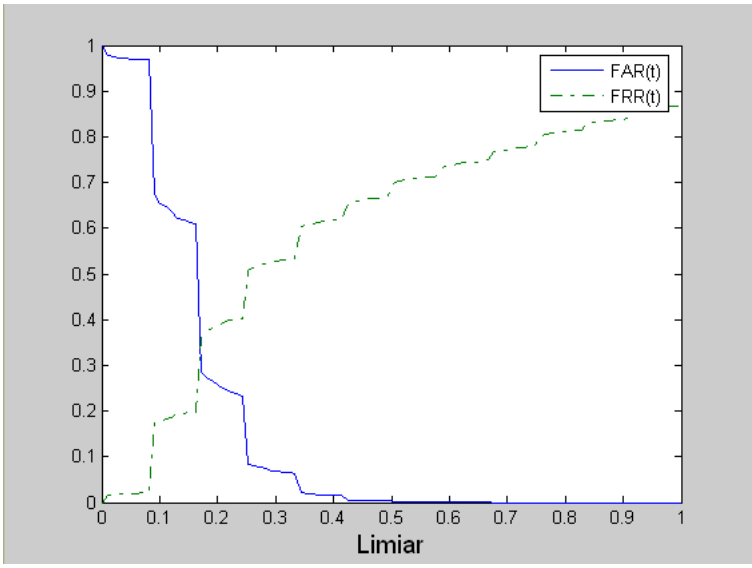


Figura B.7: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_1B

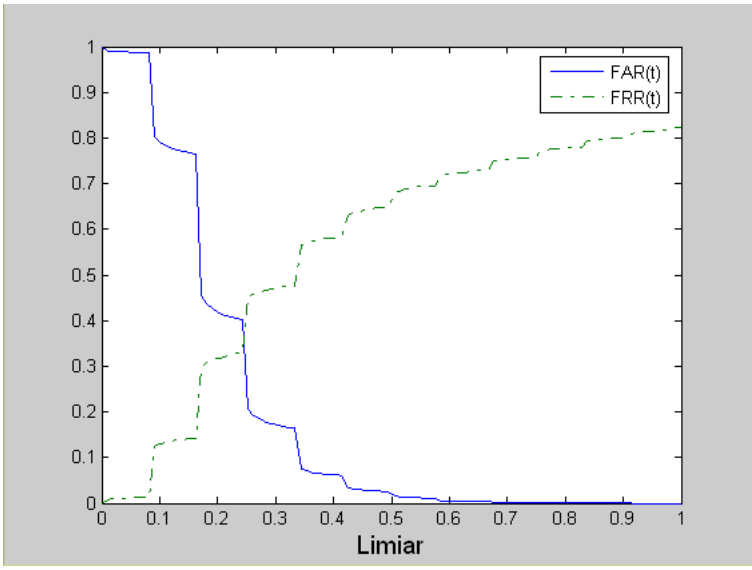


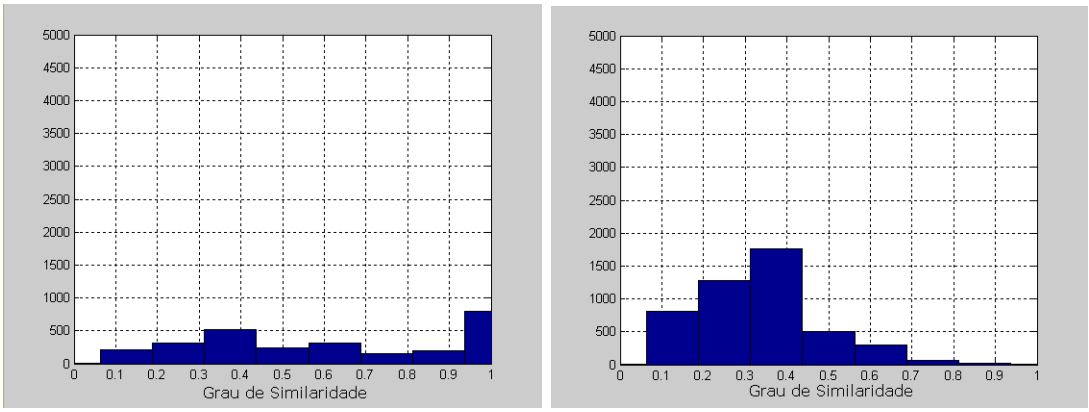
Figura B.8: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_2B

Tabela B.5: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_CENTROIDE_1C

TESTE_CENTROIDE_1C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.62	9.95	0.03s
Mediana	0.58	8.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	34.00	0.06s
Desvio Padrão	0.31	5.89	0.01s
	Reconhecimento Impostor		
Média	0.34	5.23	0.03s
Mediana	0.33	5.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	16.00	0.06s
Desvio Padrão	0.15	1.82	0.01s
$REJ_{veri} = 0.00$	$EER = 0.29$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

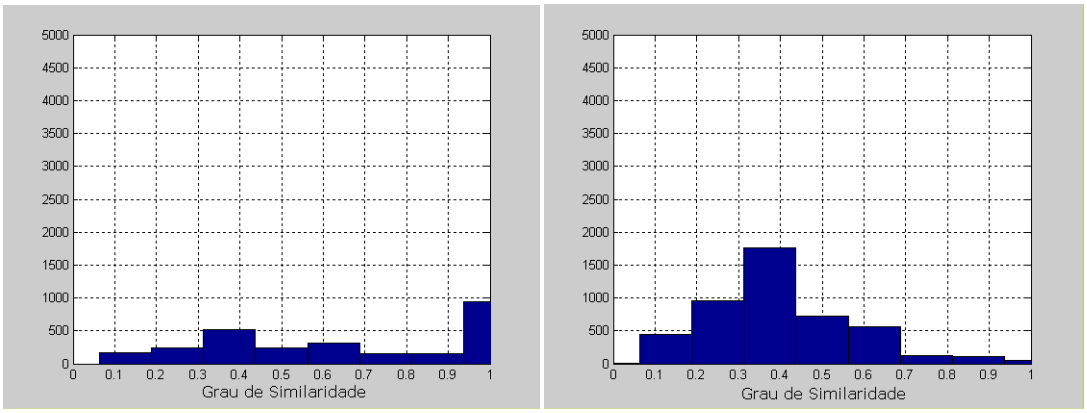
Tabela B.6: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_CENTROIDE_2C

TESTE_CENTROIDE_2C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.65	11.24	0.03s
Mediana	0.67	9.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	45.00	0.08s
Desvio Padrão	0.30	7.11	0.01s
	Reconhecimento Impostor		
Média	0.40	6.08	0.03s
Mediana	0.36	6.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	20.00	0.06s
Desvio Padrão	0.18	2.25	0.01s
$REJ_{veri} = 0.00$	$EER = 0.34$	$ZeroFAR = 1.00$	$ZeroFRR = 0.99$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.9: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_1C



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.10: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_2C

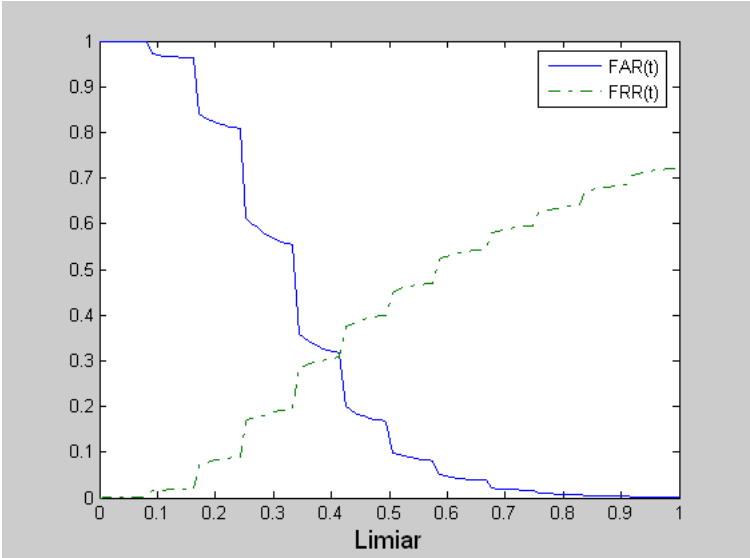


Figura B.11: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_1C

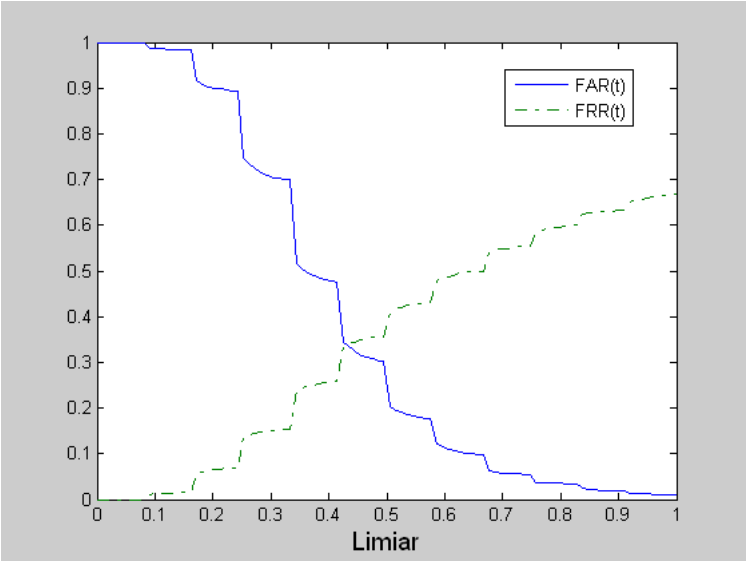


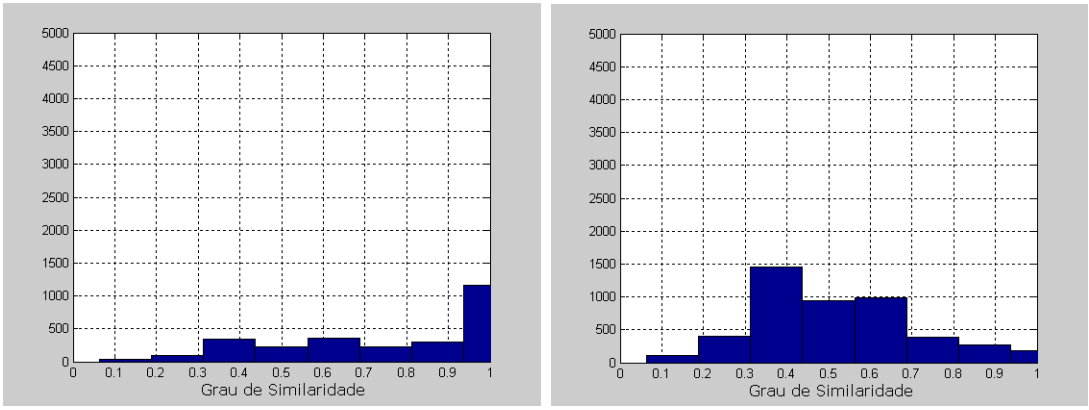
Figura B.12: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_2C

Tabela B.7: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_CENTROIDE_1D

TESTE_CENTROIDE_1D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.76	12.18	0.03s
Mediana	0.83	11.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	34.00	0.06s
Desvio Padrão	0.26	5.58	0.01s
	Reconhecimento Impostor		
Média	0.52	7.49	0.03s
Mediana	0.50	7.00	0.03s
Mínimo	0.08	2.00	0.01s
Máximo	1.00	20.00	0.06s
Desvio Padrão	0.19	2.50	0.01s
$REJ_{veri} = 0.00$	$EER = 0.30$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

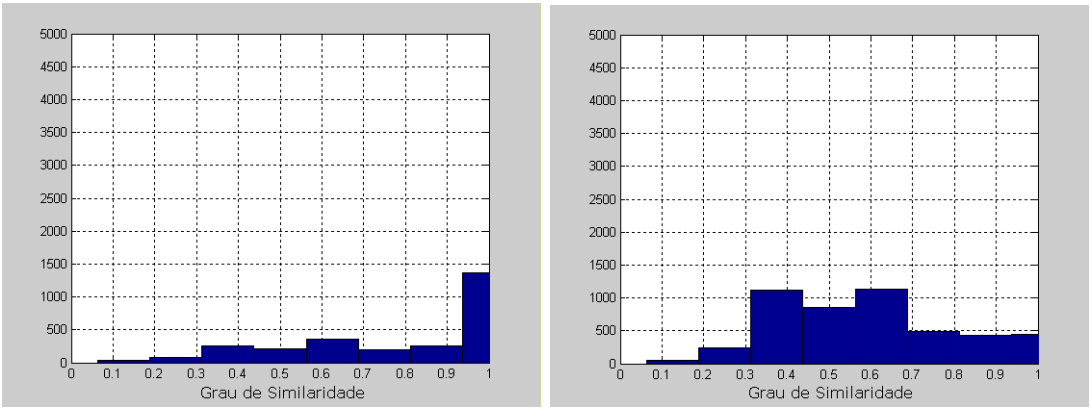
Tabela B.8: Resultados sobre o Processo de Verificação utilizando o Método Centróide com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_CENTROIDE_2D

TESTE_CENTROIDE_2D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.79	13.71	0.03s
Mediana	0.93	13.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	43.00	0.08s
Desvio Padrão	0.25	6.85	0.01s
	Reconhecimento Impostor		
Média	0.59	8.54	0.03s
Mediana	0.58	8.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	24.00	0.08s
Desvio Padrão	0.21	2.99	0.01s
$REJ_{veri} = 0.00$	$EER = 0.31$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.13: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_1D



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura B.14: Histogramas do Grau de Similaridade do TESTE_CENTROIDE_2D

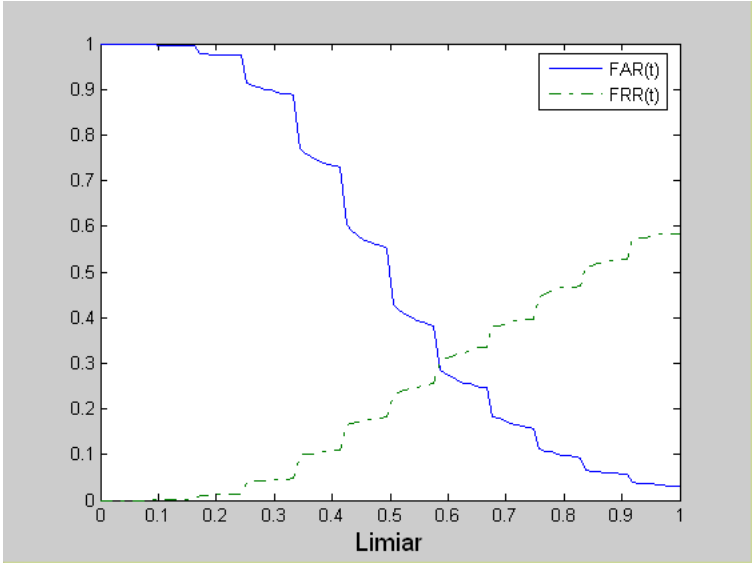


Figura B.15: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_1D

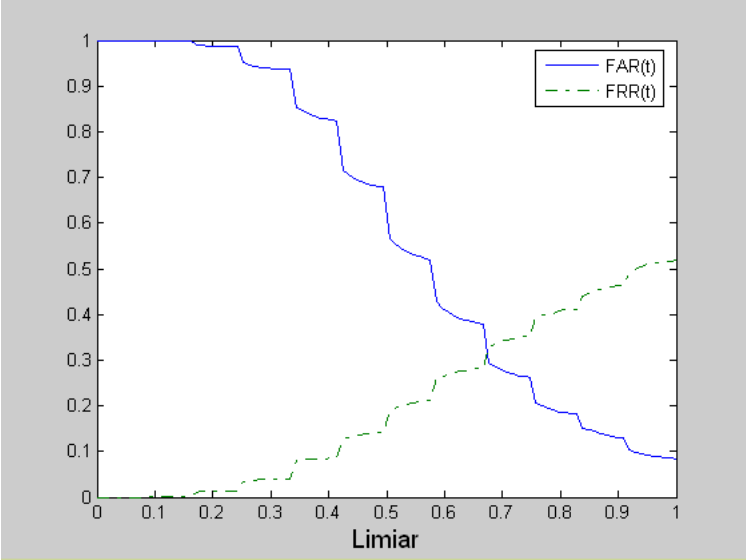


Figura B.16: Curva FAR(t) e Curva FRR(t) do TESTE_CENTROIDE_2D

APÊNDICE C - RESULTADOS - MÉTODO EXAUSTIVO

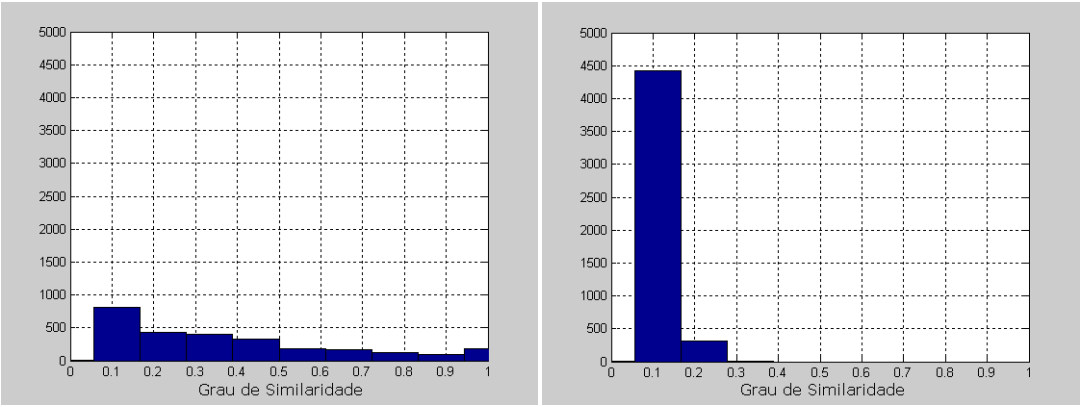
Este apêndice apresenta as estatísticas e os resultados obtidos pelo processo de verificação utilizando o método exaustivo aplicado sobre o banco DB1 do FVC de 2000.

Tabela C.1: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_EXAUSTIVO_1A

TESTE_EXAUSTIVO_1A			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.39	6.40	5.25s
Mediana	0.32	5.00	4.08s
Mínimo	0.05	2.00	0.25s
Máximo	1.00	29.00	33.69s
Desvio Padrão	0.27	3.98	4.09s
	Reconhecimento Impostor		
Média	0.14	2.72	4.95s
Mediana	0.16	3.00	4.28s
Mínimo	0.00	1.00	0.48s
Máximo	0.38	6.00	21.34s
Desvio Padrão	0.05	0.60	2.99s
$REJ_{veri} = 0.017$	$EER = 0.18$	$ZeroFAR = 0.60$	$ZeroFRR = 1.00$

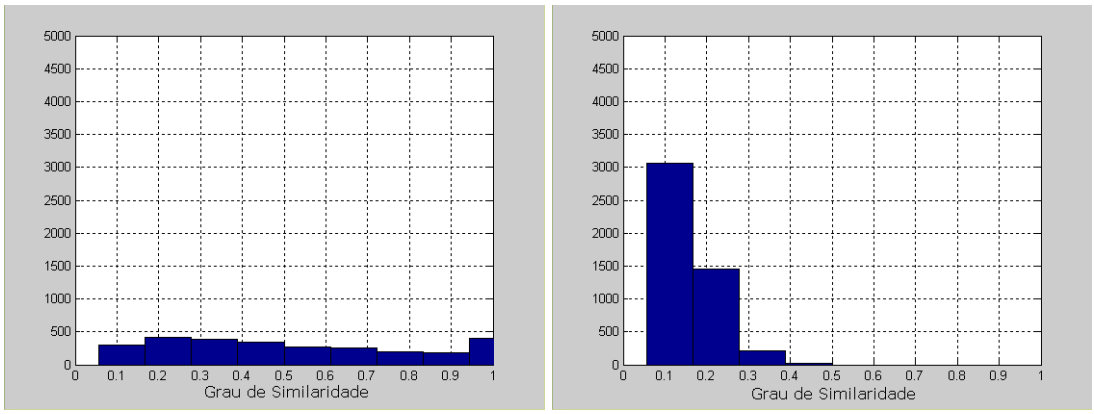
Tabela C.2: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_EXAUSTIVO_2A

TESTE_EXAUSTIVO_2A			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.53	8.43	8.36s
Mediana	0.50	8.00	6.24s
Mínimo	0.08	2.00	0.39s
Máximo	1.00	29.00	74.30s
Desvio Padrão	0.29	4.52	7.77s
	Reconhecimento Impostor		
Média	0.19	3.34	8.42s
Mediana	0.17	3.00	7.03s
Mínimo	0.08	2.00	0.53s
Máximo	0.50	7.00	48.83s
Desvio Padrão	0.06	0.74	5.69s
$REJ_{veri} = 0.133$	$EER = 0.15$	$ZeroFAR = 0.53$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.1: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_1A



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.2: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_2A

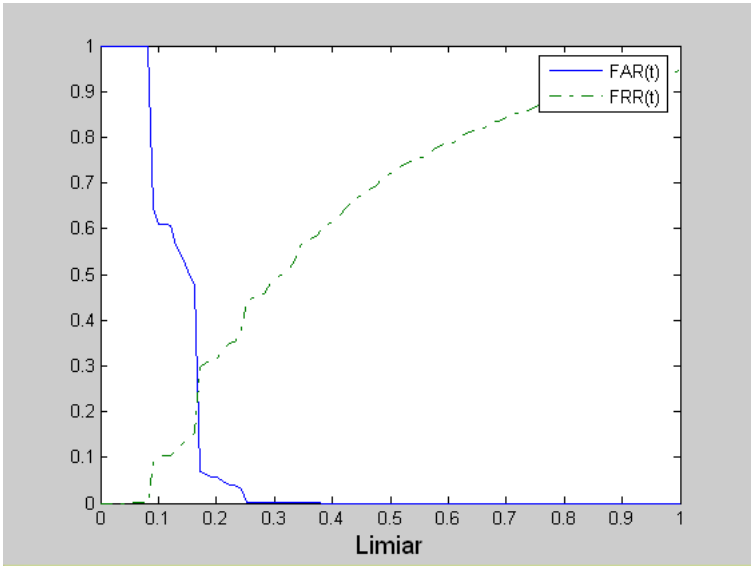


Figura C.3: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_1A

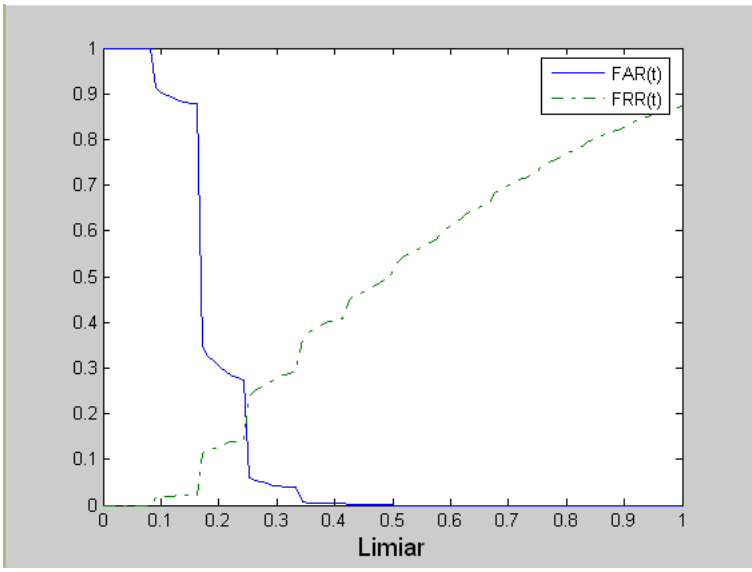


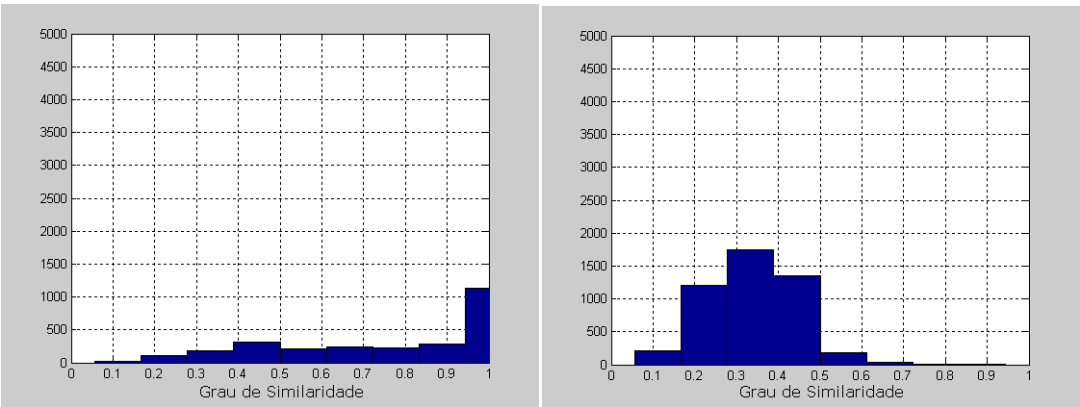
Figura C.4: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_2A

Tabela C.3: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_EXAUSTIVO_1B

TESTE_EXAUSTIVO_1B			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.76	11.66	5.23s
Mediana	0.83	12.00	4.06s
Mínimo	0.13	3.00	0.25s
Máximo	1.00	32.00	33.52s
Desvio Padrão	0.25	4.77	4.06s
	Reconhecimento Impostor		
Média	2.5	5.32	4.93s
Mediana	0.33	5.00	4.27s
Mínimo	0.08	2.00	0.48s
Máximo	0.93	13.00	21.22s
Desvio Padrão	0.10	1.28	2.98s
$REJ_{veri} = 0.016$	$EER = 0.16$	$ZeroFAR = 0.59$	$ZeroFRR = 1.00$

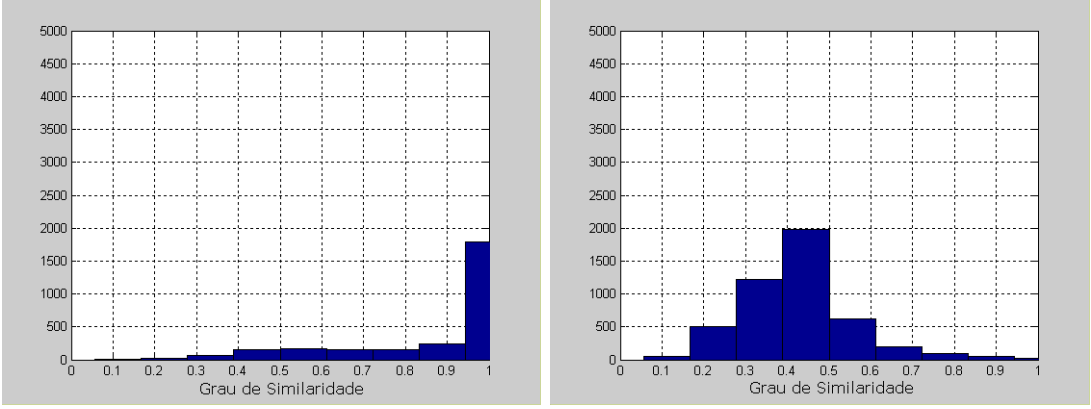
Tabela C.4: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_EXAUSTIVO_2B

TESTE_EXAUSTIVO_2B			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.88	14.47	8.32s
Mediana	1.00	14.00	6.20s
Mínimo	0.17	3.00	0.39s
Máximo	1.00	36.00	73.88s
Desvio Padrão	0.20	5.16	7.73s
	Reconhecimento Impostor		
Média	0.43	6.38	8.48s
Mediana	0.42	6.00	7.05s
Mínimo	0.17	3.00	0.55s
Máximo	1.00	17.00	52.16s
Desvio Padrão	0.13	1.66	5.71s
$REJ_{veri} = 0.132$	$EER = 0.12$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.5: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_1B



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.6: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_2B

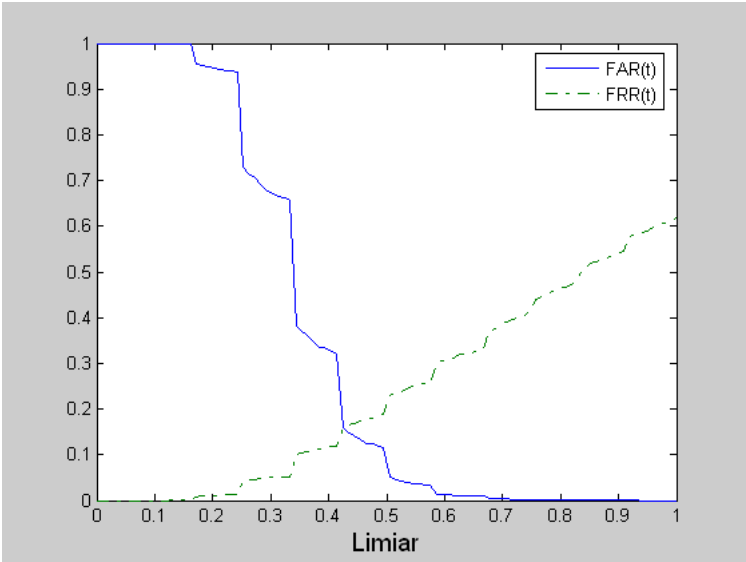


Figura C.7: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_1B

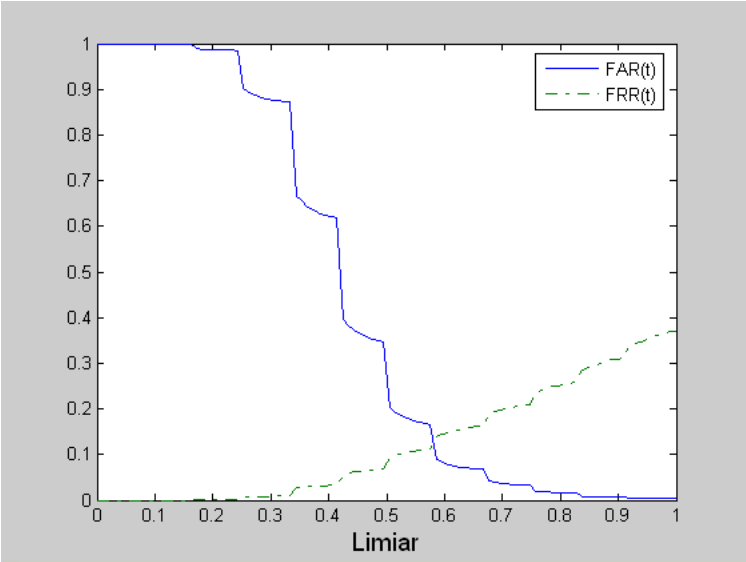


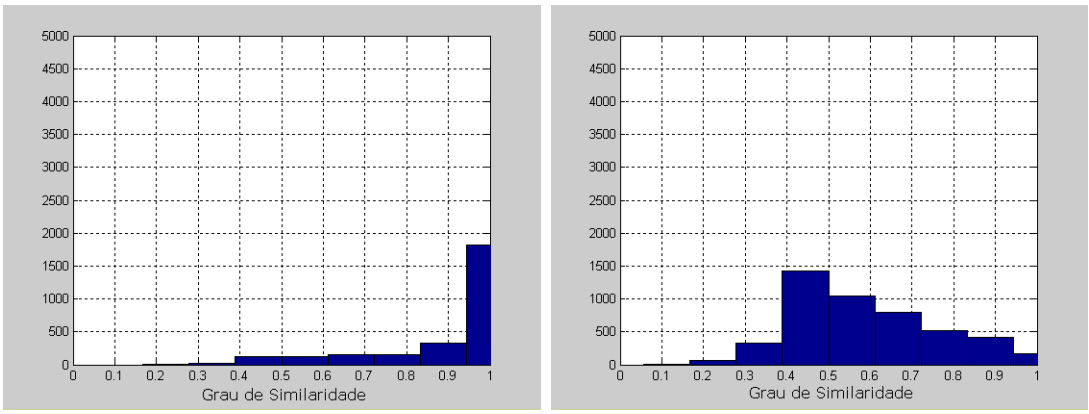
Figura C.8: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_2B

Tabela C.5: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_EXAUSTIVO_1C

TESTE_EXAUSTIVO_1C			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.90	14.03	5.17s
Mediana	1.00	14.00	4.03s
Mínimo	0.25	4.00	0.25s
Máximo	1.00	35.00	33.16s
Desvio Padrão	0.17	4.39	4.02s
	Reconhecimento Impostor		
Média	0.60	8.37	4.85s
Mediana	0.58	8.00	4.20s
Mínimo	0.17	3.00	0.48s
Máximo	1.00	18.00	20.91s
Desvio Padrão	0.17	2.14	2.92s
$REJ_{veri} = 0.015$	$EER = 0.17$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

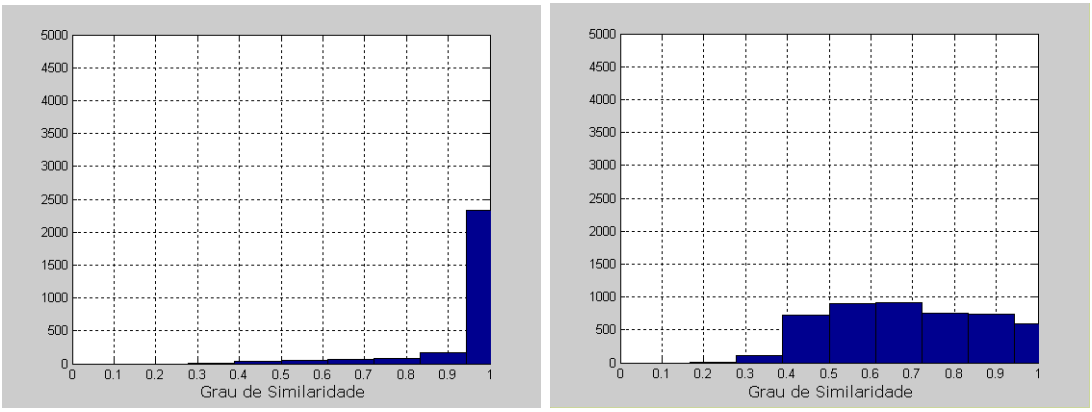
Tabela C.6: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_EXAUSTIVO_2C

TESTE_EXAUSTIVO_2C			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.96	16.89	8.38s
Mediana	1.00	16.00	6.27s
Mínimo	0.33	5.00	0.41s
Máximo	1.00	41.00	74.44s
Desvio Padrão	0.11	5.22	7.78s
	Reconhecimento Impostor		
Média	0.70	9.71	7.87s
Mediana	0.67	9.00	6.61s
Mínimo	0.25	4.00	0.55s
Máximo	1.00	20.00	44.44s
Desvio Padrão	0.18	2.39	5.18s
$REJ_{veri} = 0.116$	$EER = 0.14$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.9: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_1C



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.10: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_2C

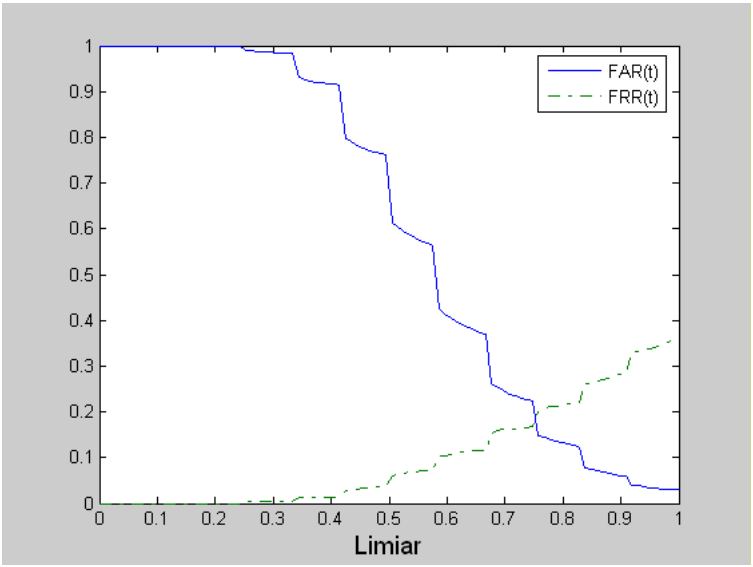


Figura C.11: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_1C

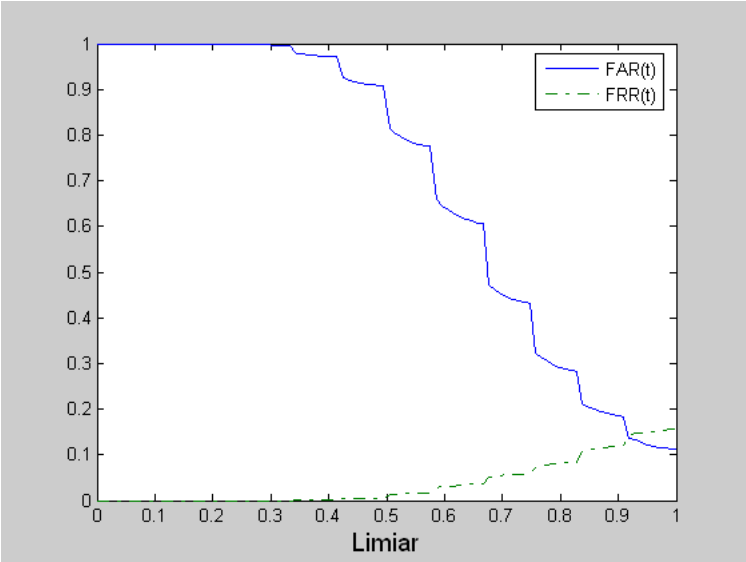


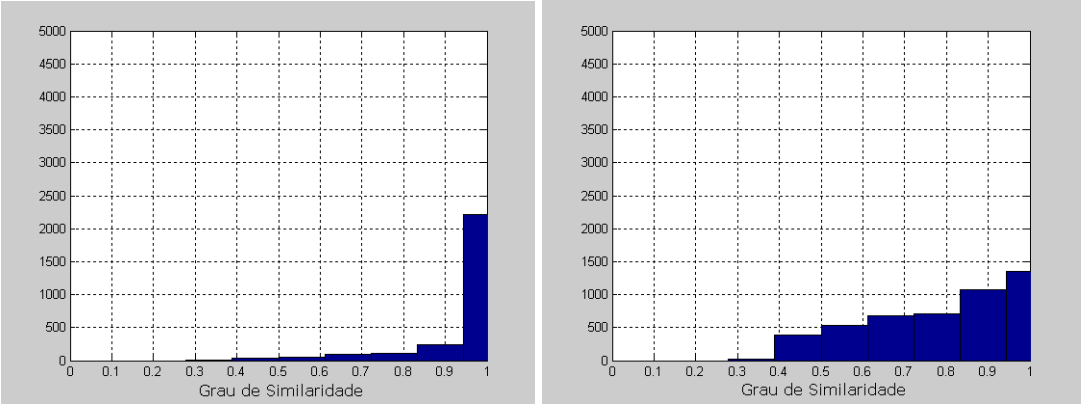
Figura C.12: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_2C

Tabela C.7: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_EXAUSTIVO_1D

TESTE_EXAUSTIVO_1D			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.95	15.21	5.11s
Mediana	1.00	14.00	4.00s
Mínimo	0.33	5.00	0.23s
Máximo	1.00	37.00	32.72s
Desvio Padrão	0.11	4.17	3.97s
	Reconhecimento Impostor		
Média	0.79	10.95	4.80s
Mediana	0.83	11.00	4.16s
Mínimo	0.33	5.00	0.47s
Máximo	1.00	23.00	20.70s
Desvio Padrão	0.18	2.47	2.89s
$REJ_{veri} = 0,014$	$EER = \emptyset$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

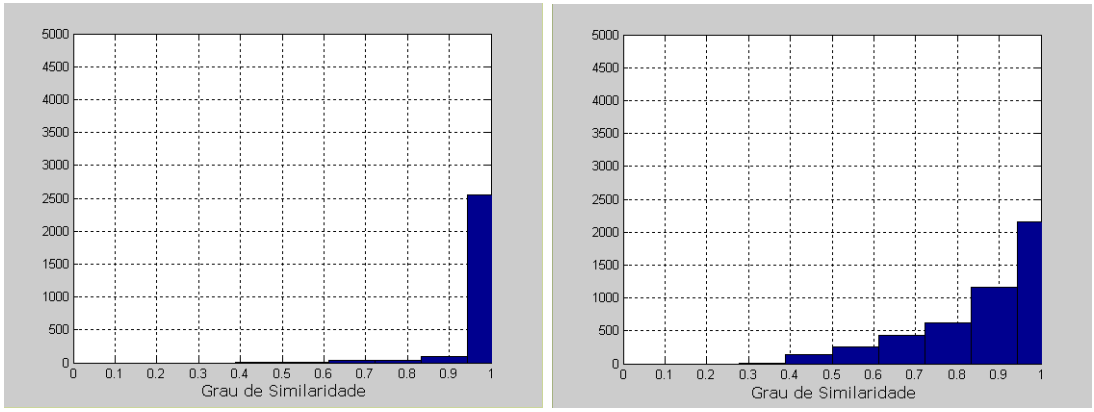
Tabela C.8: Resultados sobre o Processo de Verificação utilizando o Método Exaustivo com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_EXAUSTIVO_2D

TESTE_EXAUSTIVO_2D			
	Grau de Similiaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.98	17.67	8.41s
Mediana	1.00	16.00	6.20s
Mínimo	0.50	7.00	0.39s
Máximo	1.00	42.00	75.16s
Desvio Padrão	0.06	5.35	7.89s
	Reconhecimento Impostor		
Média	0.87	12.12	7.65s
Mediana	0.92	12.00	6.38s
Mínimo	0.33	5.00	0.50s
Máximo	1.00	22.00	44.03s
Desvio Padrão	0.15	2.37	5.11s
$REJ_{veri} = 0.114$	$EER = \emptyset$	$ZeroFAR = 1.00$	$ZeroFRR = 0.99$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.13: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_1D



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura C.14: Histogramas do Grau de Similaridade do TESTE_EXAUSTIVO_2D

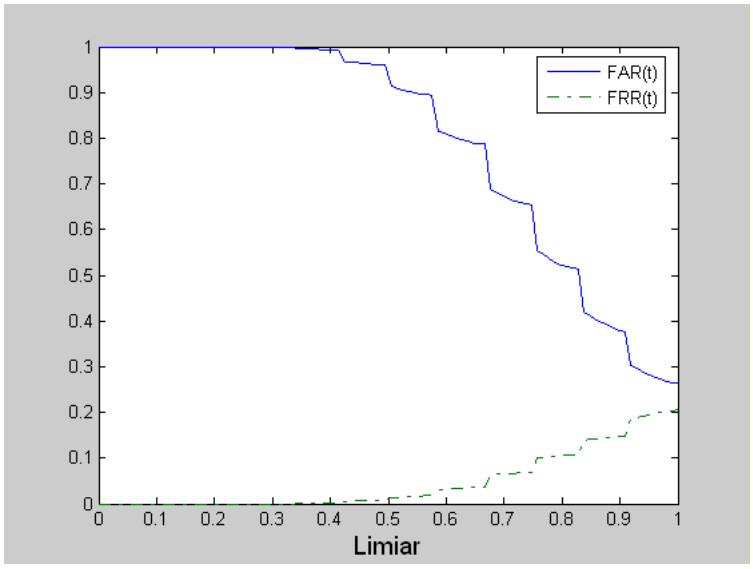


Figura C.15: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_1D

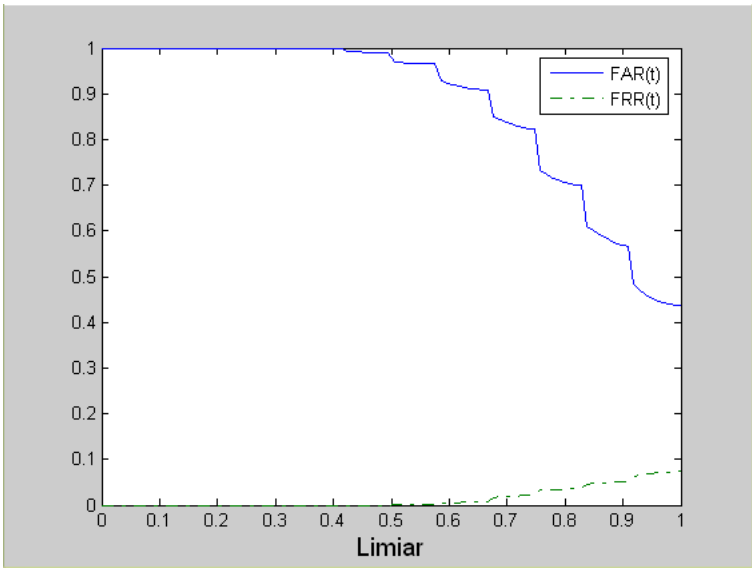


Figura C.16: Curva FAR(t) e Curva FRR(t) do TESTE_EXAUSTIVO_2D

APÊNDICE D - RESULTADOS - MÉTODO SINGULARIDADE

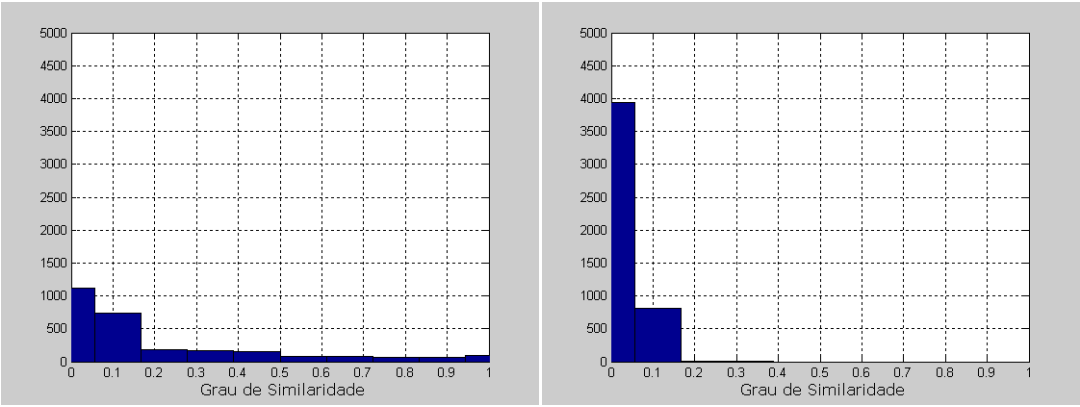
Este apêndice apresenta as estatísticas e os resultados obtidos pelo processo de verificação utilizando o método singularidade aplicado sobre o banco DB1 do FVC de 2000.

Tabela D.1: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_SINGULARIDADE_1A

TESTE_SINGULARIDADE_1A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.13	2.85	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	25.00	0.06s
Desvio Padrão	0.21	2.98	0.01s
	Reconhecimento Impostor		
Média	0.03	1.41	0.03s
Mediana	0.00	1.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.33	5.00	0.06s
Desvio Padrão	0.04	0.53	0.01s
$REJ_{veri} = 0.00$	$EER = 0.38$	$ZeroFAR = 0.89$	$ZeroFRR = 1.0$

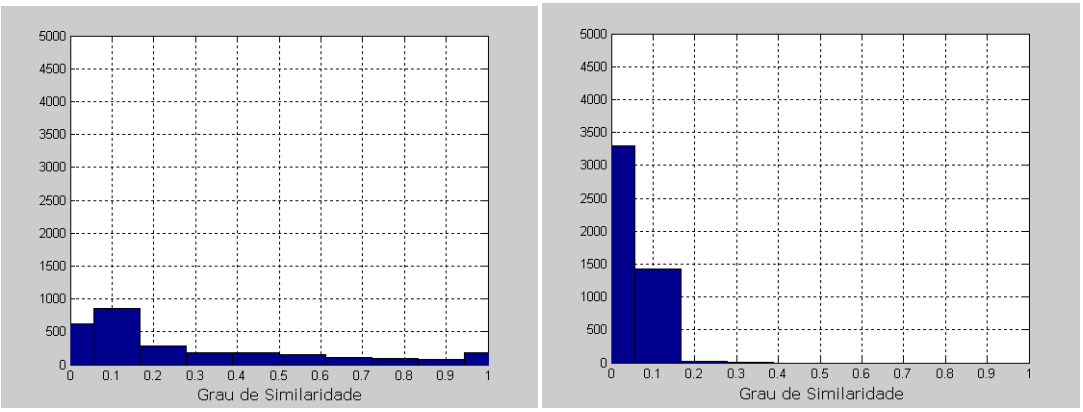
Tabela D.2: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_SINGULARIDADE_2A

TESTE_SINGULARIDADE_2A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.18	3.42	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	30.00	0.09s
Desvio Padrão	0.23	3.41	0.01s
	Reconhecimento Impostor		
Média	0.05	1.70	0.03s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	0.28	5.00	0.06s
Desvio Padrão	0.05	0.65	0.01s
$REJ_{veri} = 0.00$	$EER = 0.34$	$ZeroFAR = 0.82$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.1: Histogramas do Grau de Similaridade do TESTE_SING_1A



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.2: Histogramas do Grau de Similaridade do TESTE_SING_2A

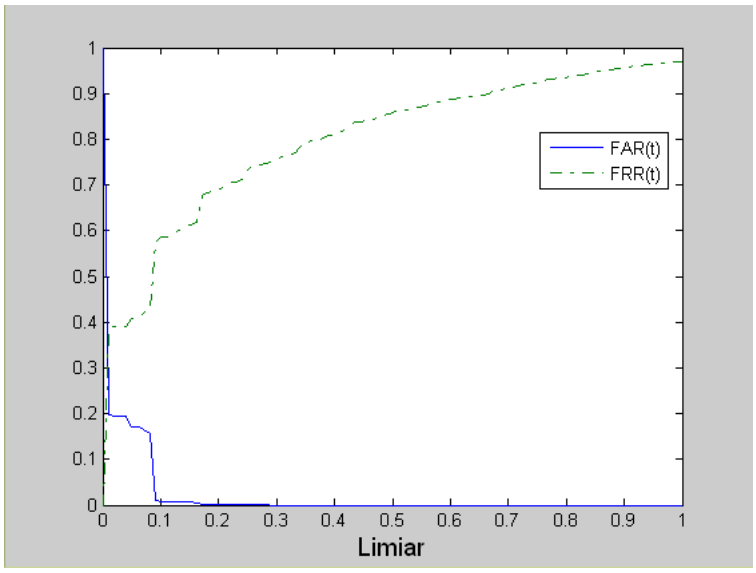


Figura D.3: Curva FAR(t) e Curva FRR(t) do TESTE_SING_1A

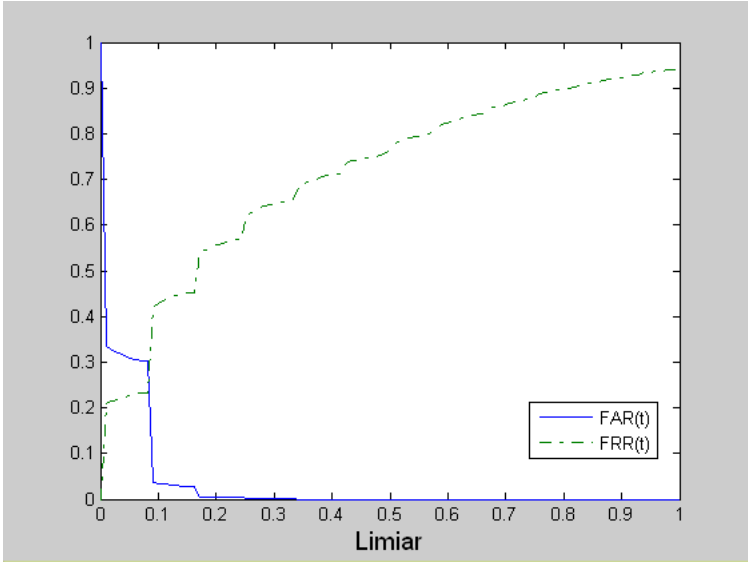


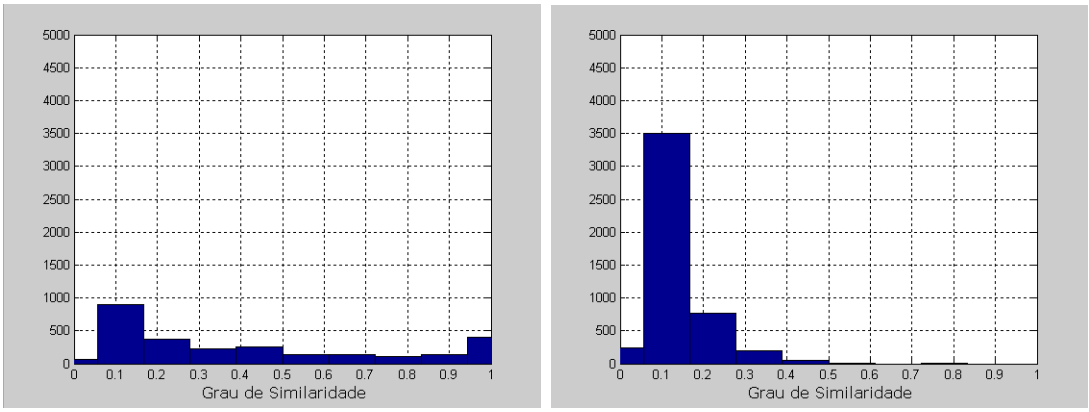
Figura D.4: Curva FAR(t) e Curva FRR(t) do TESTE_SING_2A

Tabela D.3: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_SINGULARIDADE_1B

TESTE_SINGULARIDADE_1B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.42	6.88	0.03s
Mediana	0.31	5.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	33.00	0.06s
Desvio Padrão	0.33	5.28	0.01s
	Reconhecimento Impostor		
Média	0.15	2.83	0.03s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.75	10.00	0.06s
Desvio Padrão	0.08	1.02	0.01s
$REJ_{veri} = 0.0$	$EER = 0.28$	$ZeroFAR = 0.78$	$ZeroFRR = 1.00$

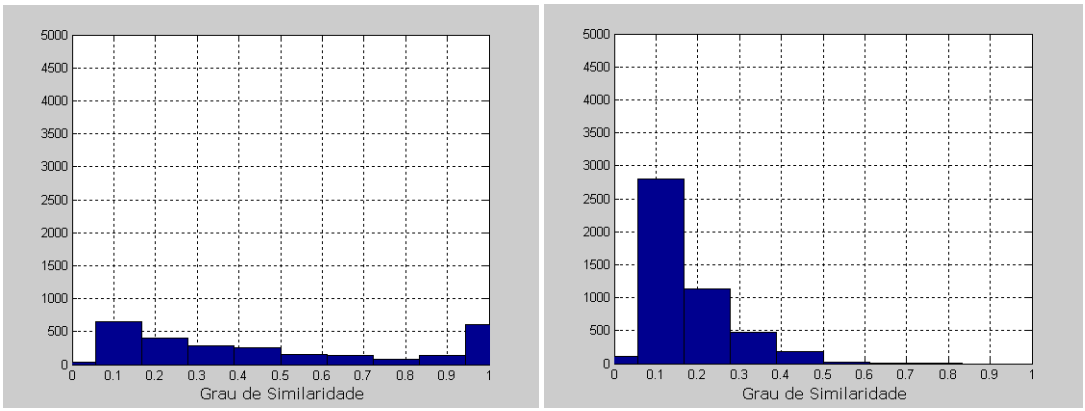
Tabela D.4: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_SINGULARIDADE_2B

TESTE_SINGULARIDADE_2B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.49	8.33	0.03s
Mediana	0.38	6.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	43.00	0.08s
Desvio Padrão	0.34	6.39	0.01s
	Reconhecimento Impostor		
Média	0.19	3.39	0.03s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.76	12.00	0.08s
Desvio Padrão	0.10	1.29	0.01s
$REJ_{veri} = 0.00$	$EER = 0.27$	$ZeroFAR = 0.72$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.5: Histogramas do Grau de Similaridade do TESTE_SING_1B



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.6: Histogramas do Grau de Similaridade do TESTE_SING_2B

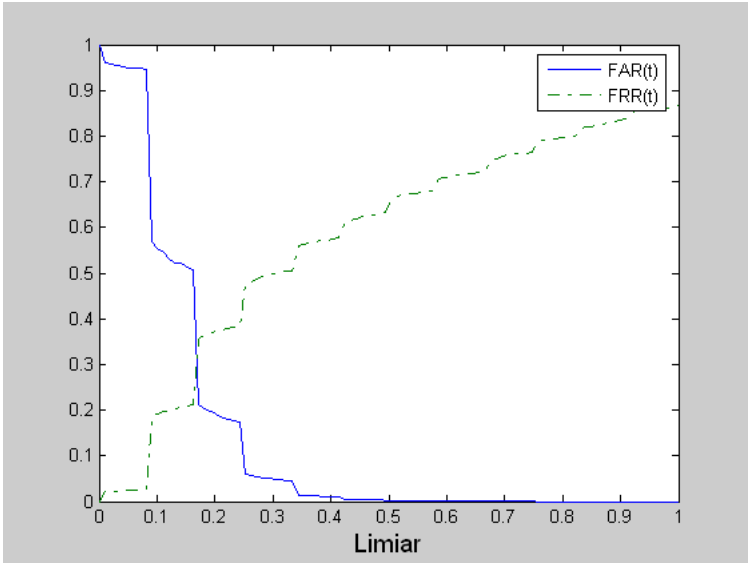


Figura D.7: Curva FAR(t) e Curva FRR(t) do TESTE_SING_1B

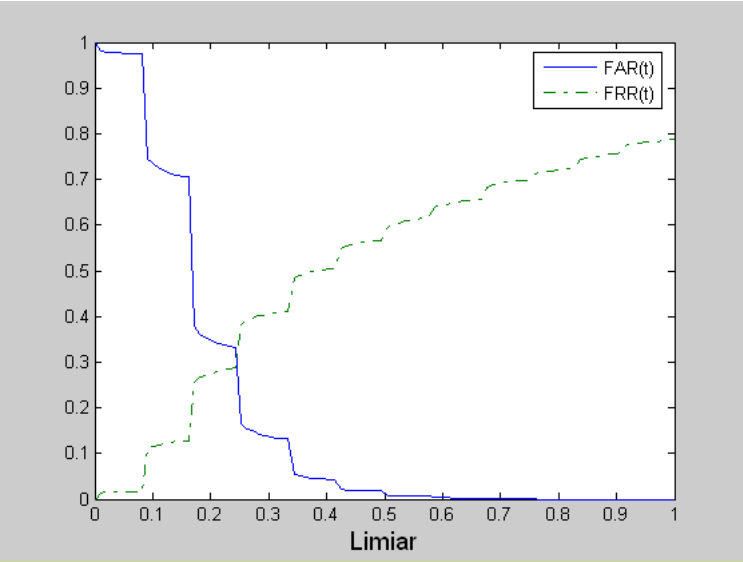


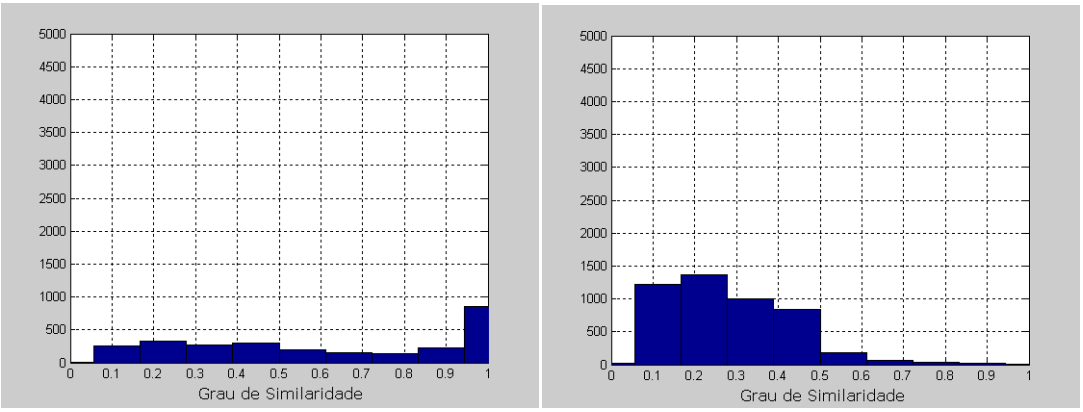
Figura D.8: Curva FAR(t) e Curva FRR(t) do TESTE_SING_2B

Tabela D.5: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_SINGULARIDADE_1C

TESTE_SINGULARIDADE_1C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.63	10.13	0.03s
Mediana	0.64	9.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	36.00	0.06s
Desvio Padrão	0.32	5.99	0.01s
	Reconhecimento Impostor		
Média	0.30	4.72	0.03s
Mediana	0.25	4.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	21.00	0.06s
Desvio Padrão	0.14	1.76	0.01s
$REJ_{veri} = 0.0$	$EER = 0.28$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

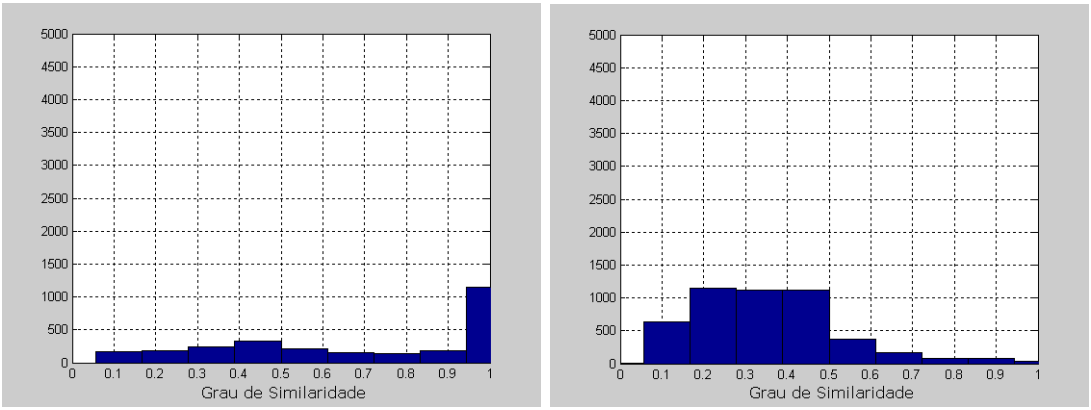
Tabela D.6: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_SINGULARIDADE_2C

TESTE_SINGULARIDADE_2C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.70	12.31	0.03s
Mediana	0.76	11.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	46.00	0.09s
Desvio Padrão	0.31	7.27	0.01s
	Reconhecimento Impostor		
Média	0.36	5.59	0.03s
Mediana	0.33	5.00	0.03s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	20.00	0.06s
Desvio Padrão	0.17	2.15	0.01s
$REJ_{veri} = 0.00$	$EER = 0.26$	$ZeroFAR = 1.00$	$ZeroFRR = 0.99$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.9: Histogramas do Grau de Similaridade do TESTE_SING_1C



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.10: Histogramas do Grau de Similaridade do TESTE_SING_2C

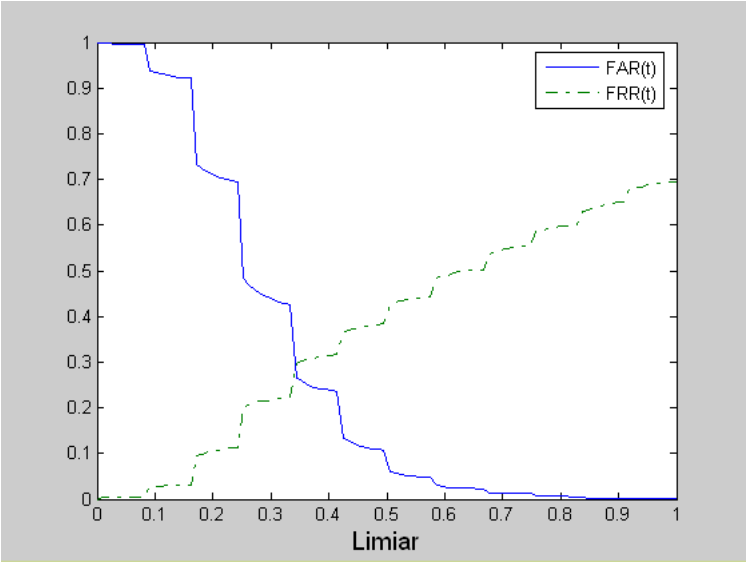


Figura D.11: Curva FAR(t) e Curva FRR(t) do TESTE_SING_1C

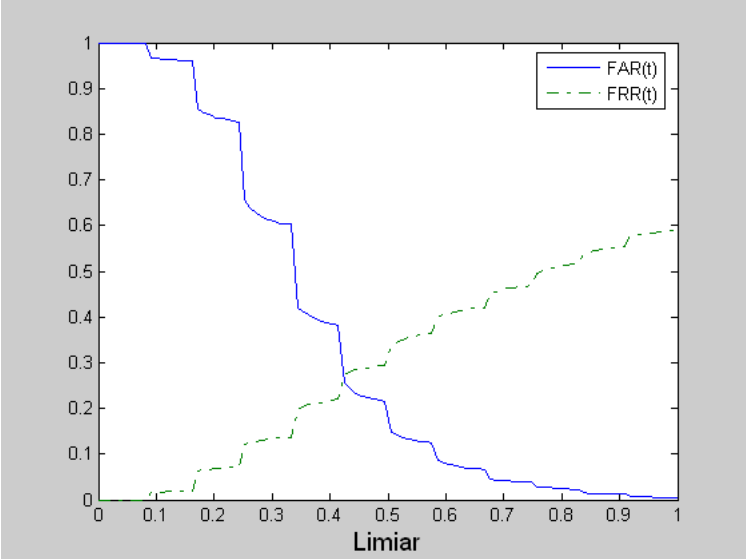


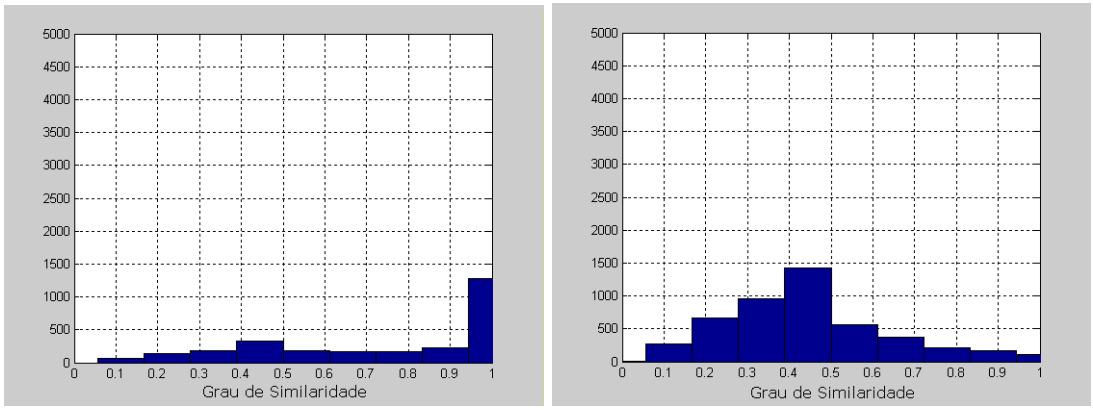
Figura D.12: Curva FAR(t) e Curva FRR(t) do TESTE_SING_2C

Tabela D.7: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_SINGULARIDADE_1D

TESTE_SINGULARIDADE_1D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.76	12.40	0.03s
Mediana	0.92	12.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	38.00	0.06s
Desvio Padrão	0.28	6.08	0.01s
	Reconhecimento Impostor		
Média	0.46	6.71	0.03s
Mediana	0.42	6.00	0.03s
Mínimo	0.04	2.00	0.01s
Máximo	1.00	19.00	0.05s
Desvio Padrão	0.19	2.45	0.01s
$REJ_{veri} = 0.00$	$EER = 0.28$	$ZeroFAR = 1.00$	$ZeroFRR = 0.99$

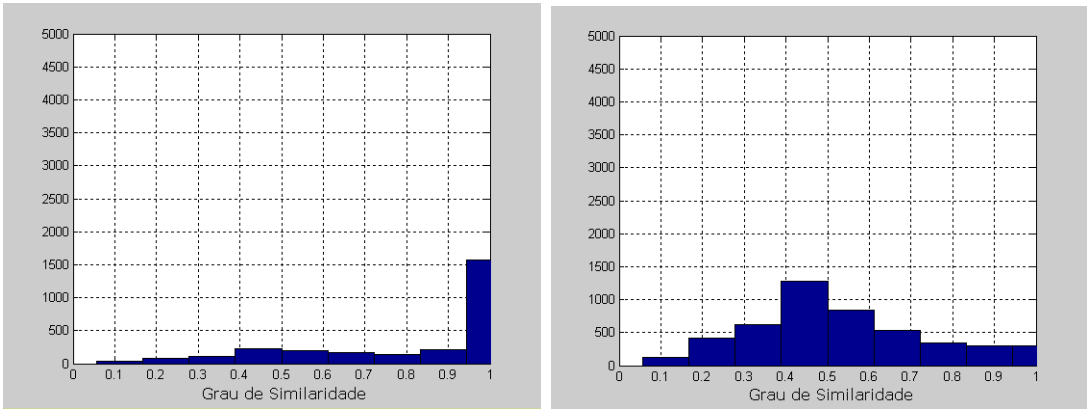
Tabela D.8: Resultados sobre o Processo de Verificação utilizando o Método Singularidade com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_SINGULARIDADE_2D

TESTE_SINGULARIDADE_2D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.82	14.85	0.03s
Mediana	1.00	14.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	51.00	0.08s
Desvio Padrão	0.25	7.25	0.01s
	Reconhecimento Impostor		
Média	0.54	7.89	0.03s
Mediana	0.50	8.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	24.00	0.06s
Desvio Padrão	0.21	2.88	0.01s
$REJ_{veri} = 0.00$	$EER = 0.25$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.13: Histogramas do Grau de Similaridade do TESTE_SING_1D



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura D.14: Histogramas do Grau de Similaridade do TESTE_SING_2D

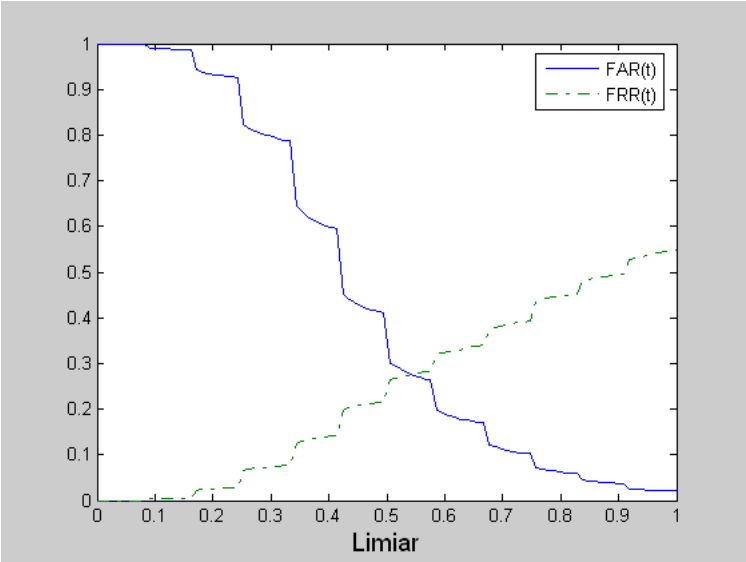


Figura D.15: Curva FAR(t) e Curva FRR(t) do TESTE_SING_1D

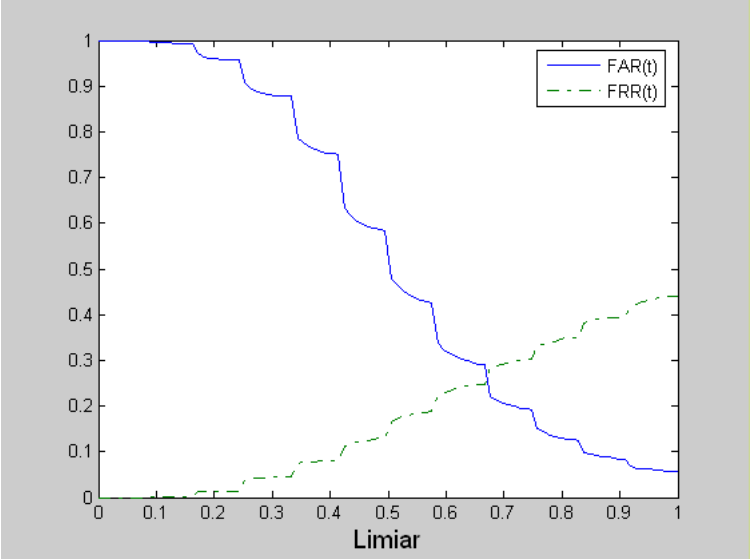


Figura D.16: Curva FAR(t) e Curva FRR(t) do TESTE_SING_2D

APÊNDICE E - RESULTADOS - MÉTODO CARACTERÍSTICAS LOCAIS

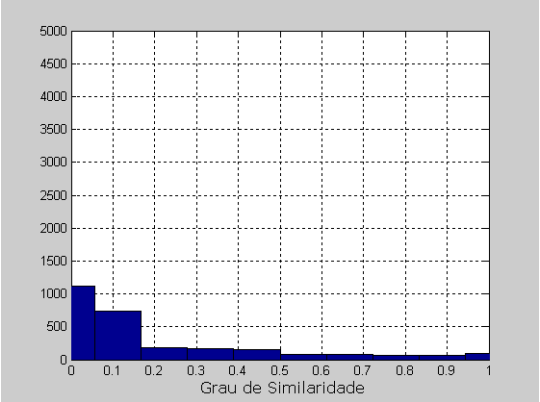
Este apêndice apresenta as estatísticas e os resultados obtidos pelo processo de verificação utilizando o método características locais aplicado sobre o banco DB1 do FVC de 2000.

Tabela E.1: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_CARAC.LOCAIS_1A

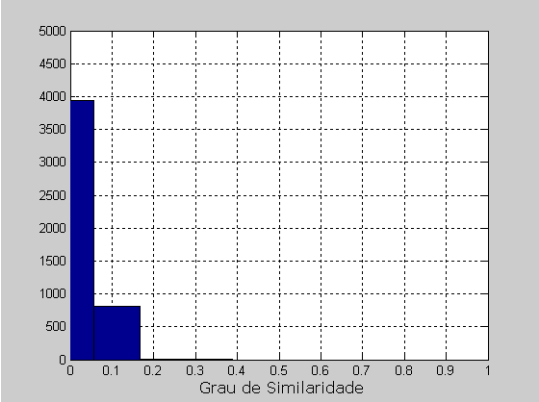
TESTE_CARAC.LOCAIS_1A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.20	3.81	0.05s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	31.00	0.42s
Desvio Padrão	0.27	4.02	0.05s
	Reconhecimento Impostor		
Média	0.02	1.22	0.05s
Mediana	0.00	1.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.29	5.00	0.30s
Desvio Padrão	0.03	0.44	0.03s
$REJ_{veri} = 0.00$	$EER = 0.29$	$ZeroFAR = 0.75$	$ZeroFRR = 1.00$

Tabela E.2: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 10$ e $\Delta\theta = 10$ - TESTE_CARAC.LOCAIS_2A

TESTE_CARAC.LOCAIS_2A			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.29	5.08	0.05s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	28.00	0.95s
Desvio Padrão	0.30	4.64	0.08s
	Reconhecimento Impostor		
Média	0.03	1.40	0.05s
Mediana	0.00	1.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.33	5.00	0.53s
Desvio Padrão	0.05	0.59	0.05s
$REJ_{veri} = 0.00$	$EER = 0.23$	$ZeroFAR = 0.69$	$ZeroFRR = 1.00$

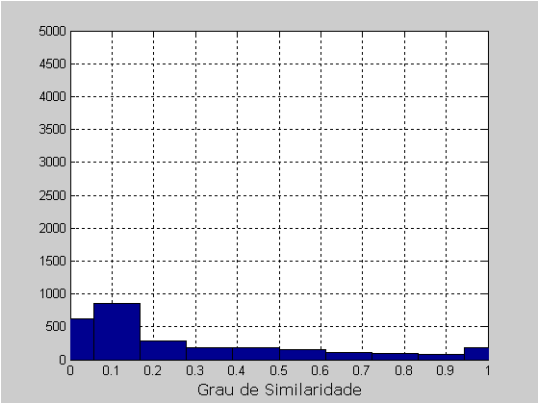


(a) Distribuição Genuíno

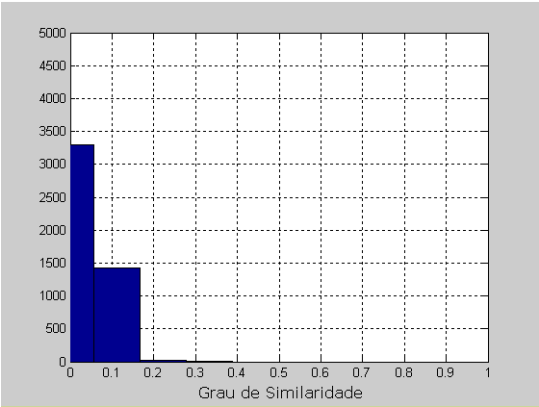


(b) Distribuição Impostor

Figura E.1: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_1A



(a) Distribuição Genuíno



(b) Distribuição Impostor

Figura E.2: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_2A

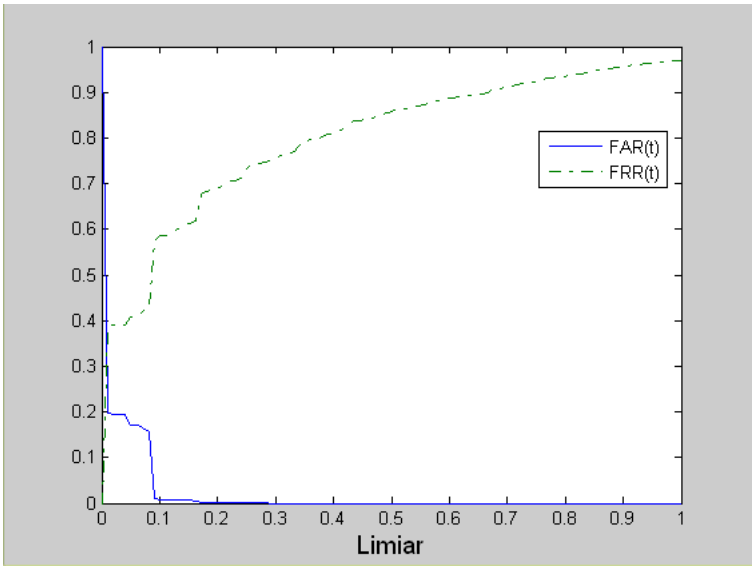


Figura E.3: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_1A

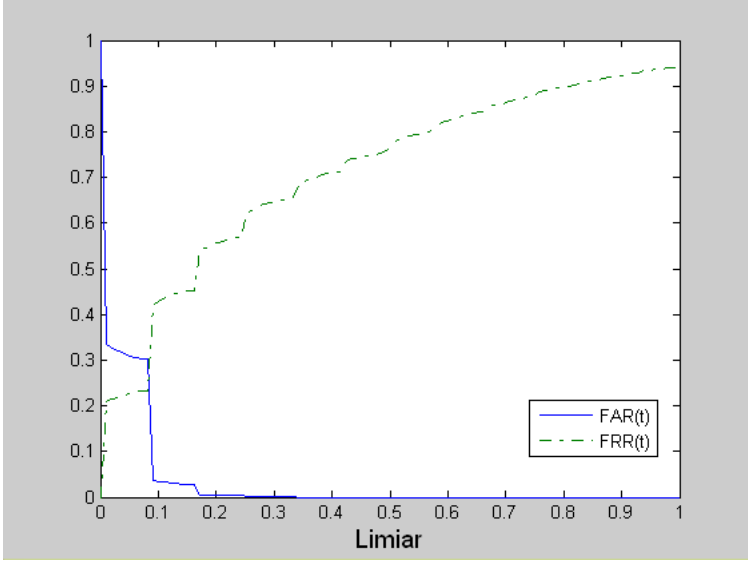


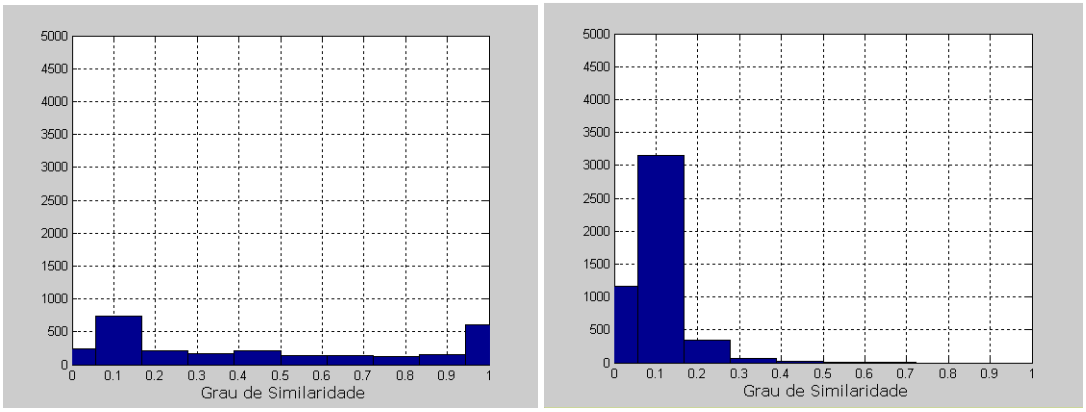
Figura E.4: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_2A

Tabela E.3: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_CARAC.LOCAIS_1B

TESTE_CARAC.LOCAIS_1B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.47	7.85	0.05s
Mediana	0.42	6.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	33.00	0.42s
Desvio Padrão	0.37	6.20	0.04s
	Reconhecimento Impostor		
Média	0.10	2.25	0.05s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.67	9.00	0.27s
Desvio Padrão	0.08	0.97	0.03s
$REJ_{veri} = 0.00$	$EER = 0.22$	$ZeroFAR = 0.66$	$ZeroFRR = 1.00$

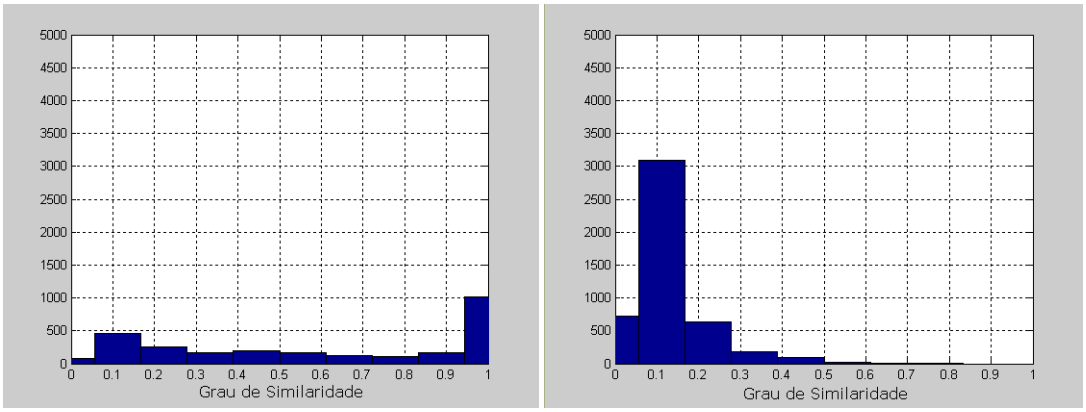
Tabela E.4: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 20$ e $\Delta\theta = 20$ - TESTE_CARAC.LOCAIS_2B

TESTE_CARAC.LOCAIS_2B			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.61	10.73	0.05s
Mediana	0.67	9.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	42.00	1.14s
Desvio Padrão	0.36	7.43	0.08s
	Reconhecimento Impostor		
Média	0.13	2.69	0.05s
Mediana	0.08	2.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	0.83	11.00	0.55s
Desvio Padrão	0.10	1.23	0.05s
$REJ_{veri} = 0.00$	$EER = 0.20$	$ZeroFAR = 0.58$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.5: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_1B



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.6: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_2B

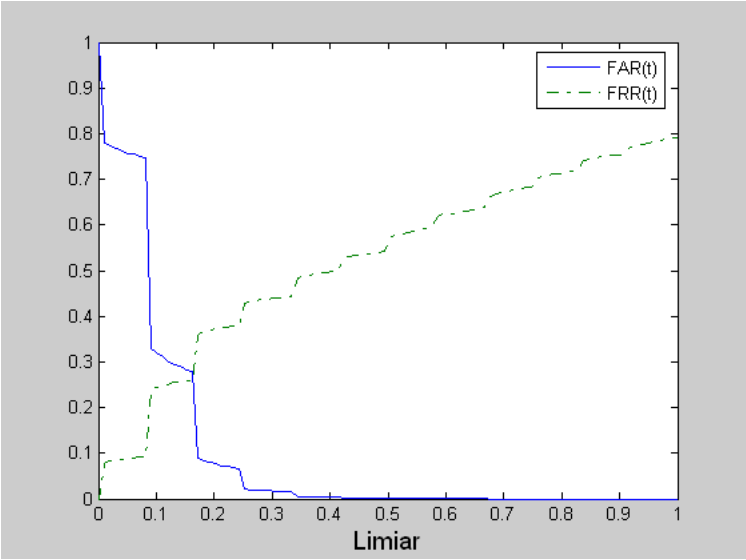


Figura E.7: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_1B

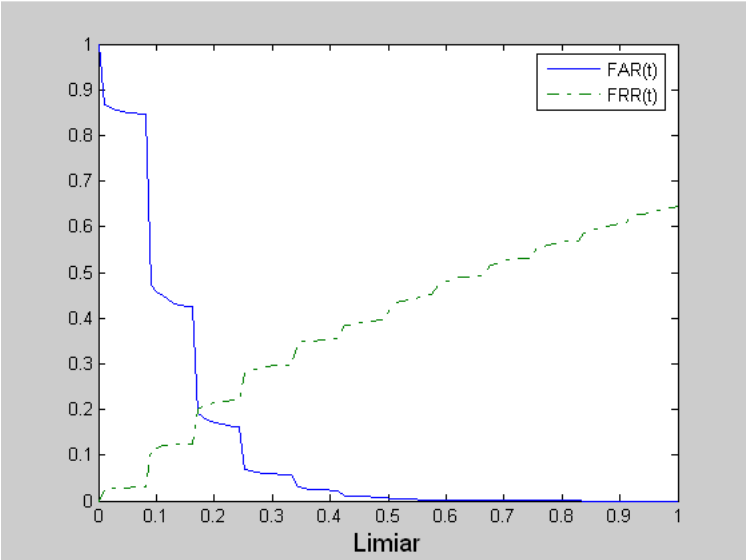


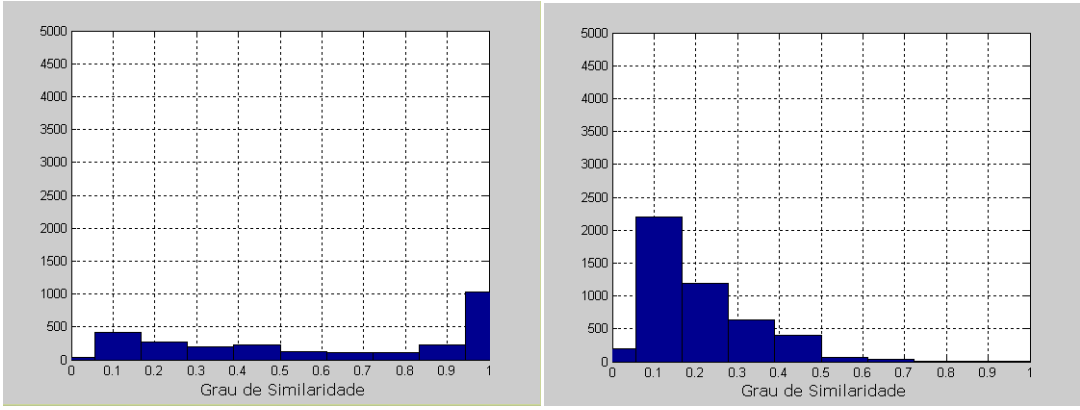
Figura E.8: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_2B

Tabela E.5: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_CARAC.LOCAIS_1C

TESTE_CARAC.LOCAIS_1C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.64	10.69	0.05s
Mediana	0.71	10.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	35.00	0.44s
Desvio Padrão	2.5	6.86	0.05s
	Reconhecimento Impostor		
Média	0.22	3.75	0.05s
Mediana	0.17	3.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	13.00	0.28s
Desvio Padrão	0.13	1.63	0.03s
$REJ_{veri} = 0.00$	$EER = 0.26$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

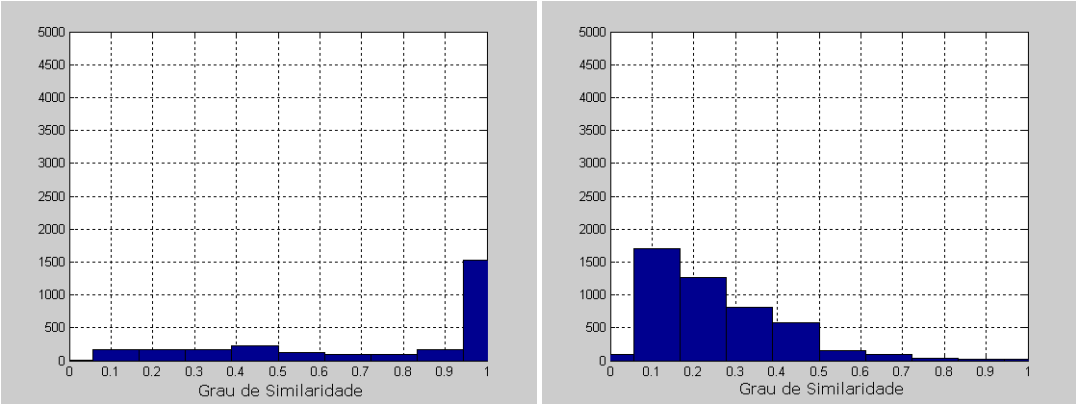
Tabela E.6: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ - TESTE_CARAC.LOCAIS_2C

TESTE_CARAC.LOCAIS_2C			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.77	14.34	0.05s
Mediana	1.00	14.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	47.00	1.14s
Desvio Padrão	0.31	8.09	0.08s
	Reconhecimento Impostor		
Média	0.27	4.41	0.05s
Mediana	0.25	4.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	18.00	0.55s
Desvio Padrão	0.16	2.01	0.05s
$REJ_{veri} = 0.00$	$EER = 0.19$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.9: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_1C



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.10: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_2C

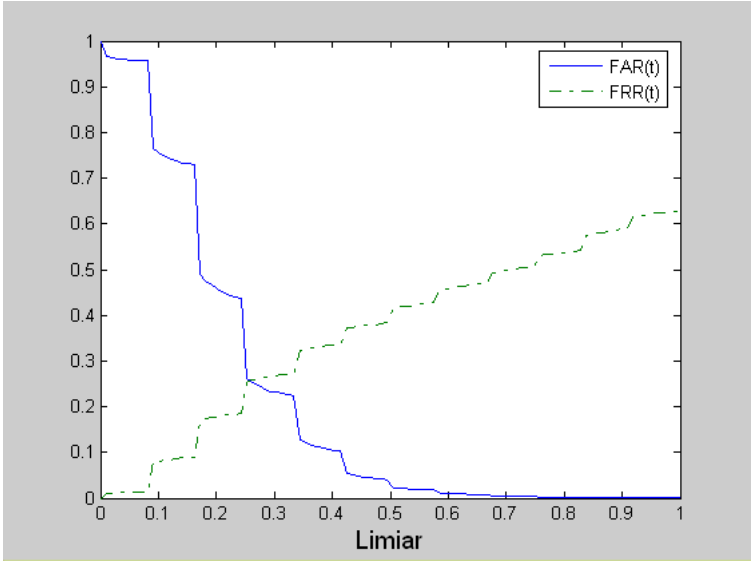


Figura E.11: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_1C

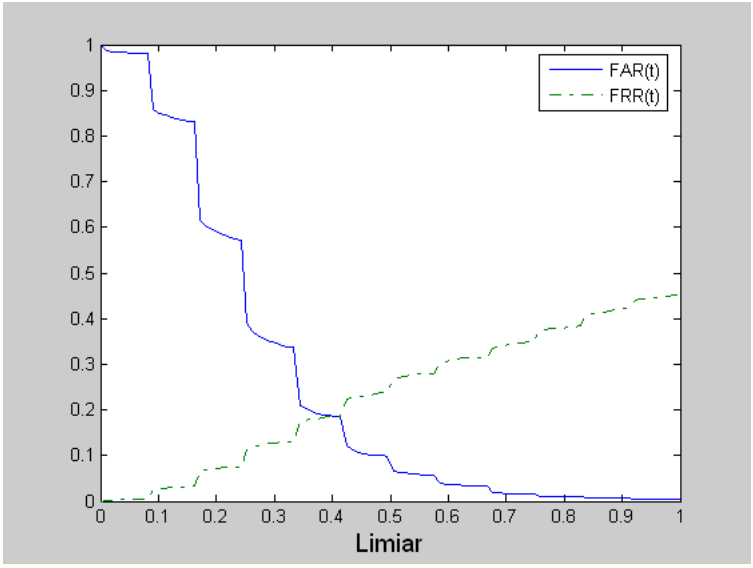


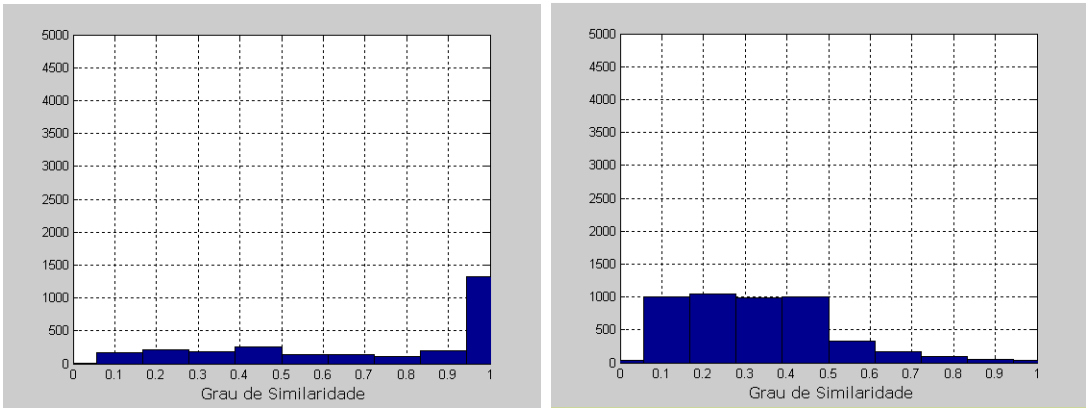
Figura E.12: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_2C

Tabela E.7: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_CARAC.LOCAIS_1D

TESTE_CARAC.LOCAIS_1D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.73	12.62	0.05s
Mediana	0.92	12.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	37.00	0.44s
Desvio Padrão	0.31	6.98	0.04s
	Reconhecimento Impostor		
Média	0.34	5.29	0.05s
Mediana	0.33	5.00	0.03s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	18.00	0.28s
Desvio Padrão	0.18	2.24	0.03s
$REJ_{veri} = 0.00$	$EER = 0.25$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

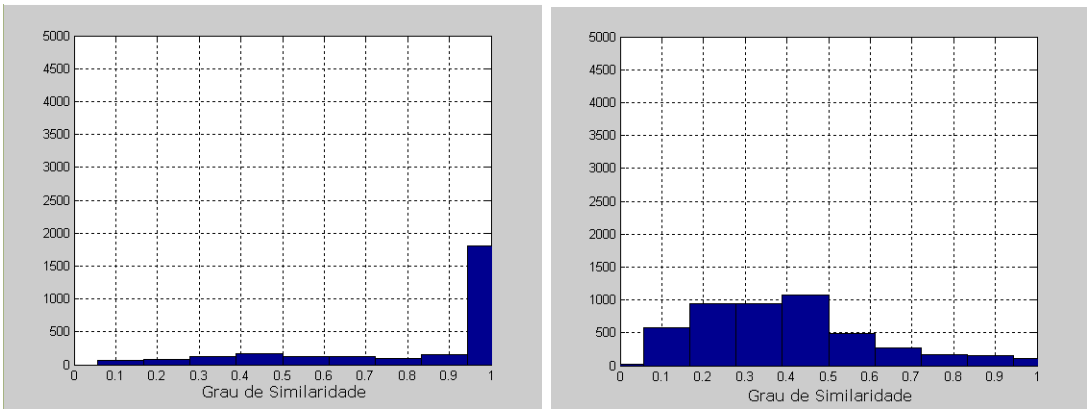
Tabela E.8: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 40$ e $\Delta\theta = 40$ - TESTE_CARAC.LOCAIS_2D

TESTE_CARAC.LOCAIS_2D			
	Grau de Similaridade	Número Minúcias Equivalentes	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.85	16.60	0.06s
Mediana	1.00	16.00	0.03s
Mínimo	0.08	2.00	0.00s
Máximo	1.00	48.00	1.17s
Desvio Padrão	0.25	8.14	0.09s
	Reconhecimento Impostor		
Média	0.41	6.22	0.06s
Mediana	0.36	6.00	0.05s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	21.00	0.50s
Desvio Padrão	0.21	2.72	0.06s
$REJ_{veri} = 0.00$	$EER = 0.18$	$ZeroFAR = 1.00$	$ZeroFRR = 0.99$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.13: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_1D



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura E.14: Histogramas do Grau de Similaridade do TESTE_CAR.LOCAIS_2D

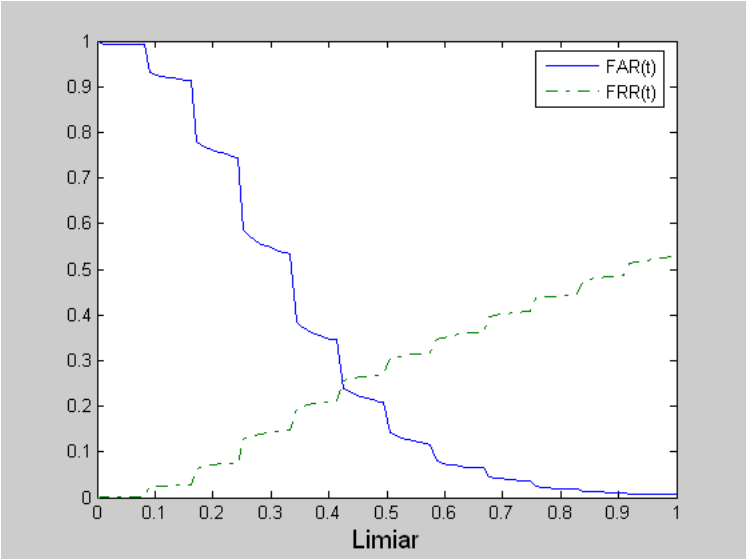


Figura E.15: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_1D

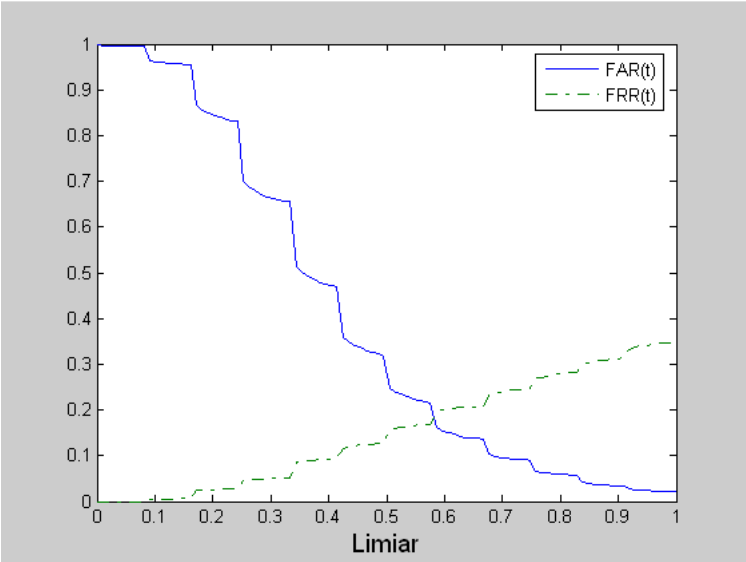


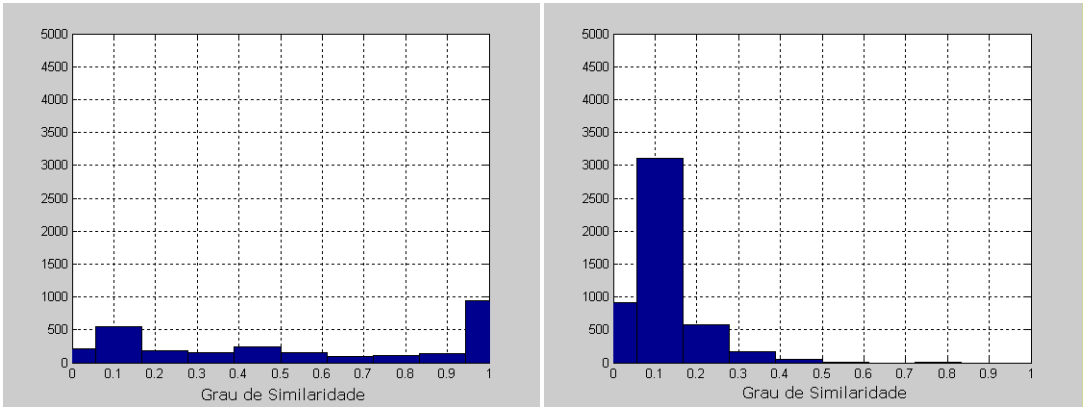
Figura E.16: Curva FAR(t) e Curva FRR(t) do TESTE_CAR.LOCAIS_2D

APÊNDICE F - RESULTADOS - DEMAIS BANCOS DO FVC

Este apêndice apresenta as estatísticas e os resultados obtidos pelo processo de verificação utilizando o método características locais aplicado sobre os demais bancos do do FVC de 2000, 2002 e 2004.

Tabela F.1: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB2 FVC/2000

TESTE_CAR.LOCAIS_2000DB2			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.57	9.99	0.07s
Mediana	0.58	8.00	0.05s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	43.00	1.31s
Desvio Padrão	0.38	7.70	0.10s
	Reconhecimento Impostor		
Média	0.12	2.53	0.06s
Mediana	0.08	2.00	0.05s
Mínimo	0.00	1.00	0.00s
Máximo	0.75	10.00	0.34s
Desvio Padrão	0.09	1.17	0.05s
$REJ_{veri} = 0$	$EER = 0.22$	$ZeroFAR = 0.59$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.1: Histogramas do Grau de Similaridade do Banco DB2 FVC/2000

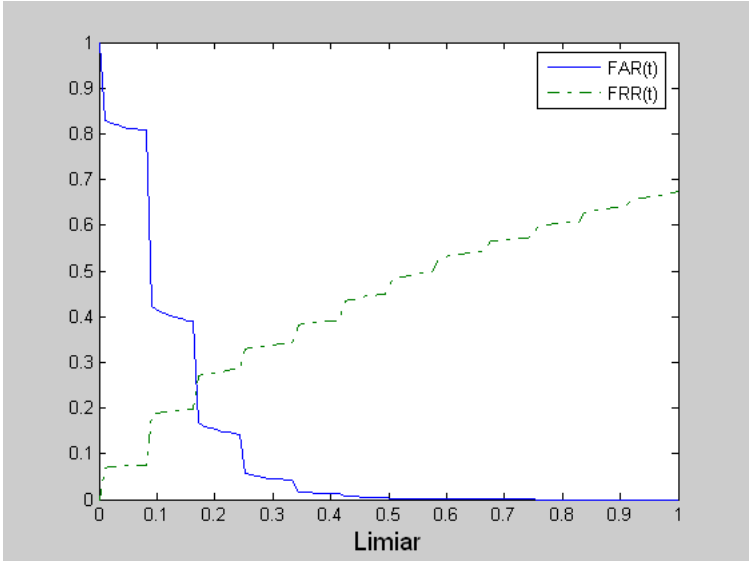
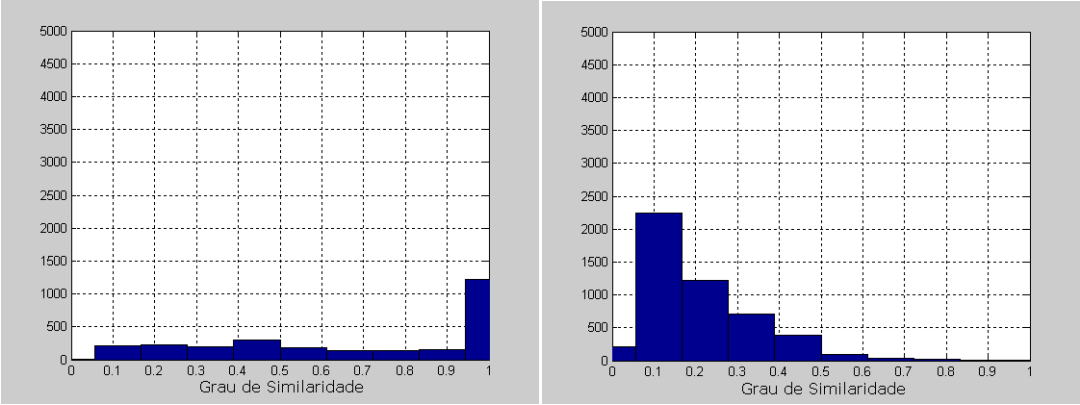


Figura F.2: Curva FAR(t) e Curva FRR(t) do Banco DB2 FVC/2000



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.3: Histogramas do Grau de Similaridade do Banco DB3 FVC/2000

Tabela F.2: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB3 FVC/2000

TESTE_CAR.LOCAIS_2000DB3			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.70	13.99	6.02s
Mediana	0.81	11.00	1.07s
Mínimo	0.00	1.00	0.05s
Máximo	1.00	64.00	335.14s
Desvio Padrão	0.32	10.11	20.51s
	Reconhecimento Impostor		
Média	0.22	3.83	1.76s
Mediana	0.17	4.00	0.94s
Mínimo	0.00	1.00	0.08s
Máximo	1.00	15.00	73.23s
Desvio Padrão	0.14	1.75	3.20s
$REJ_{veri} = 0.043$	$EER = 0.17$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

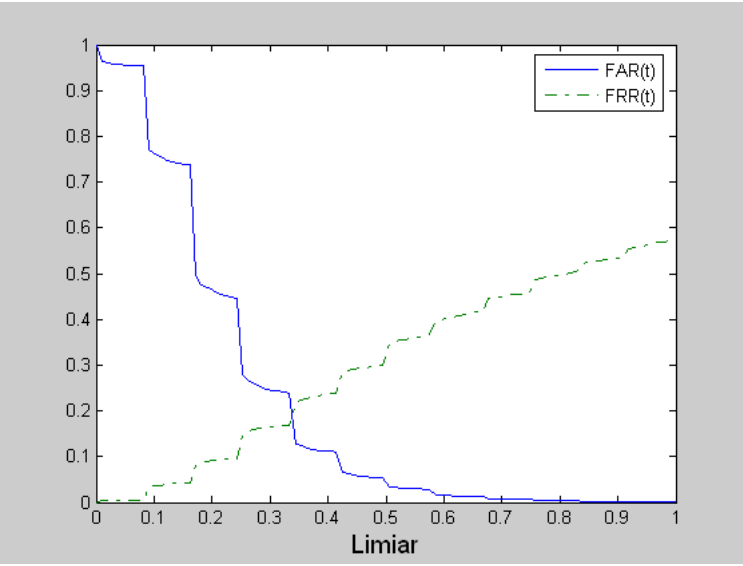
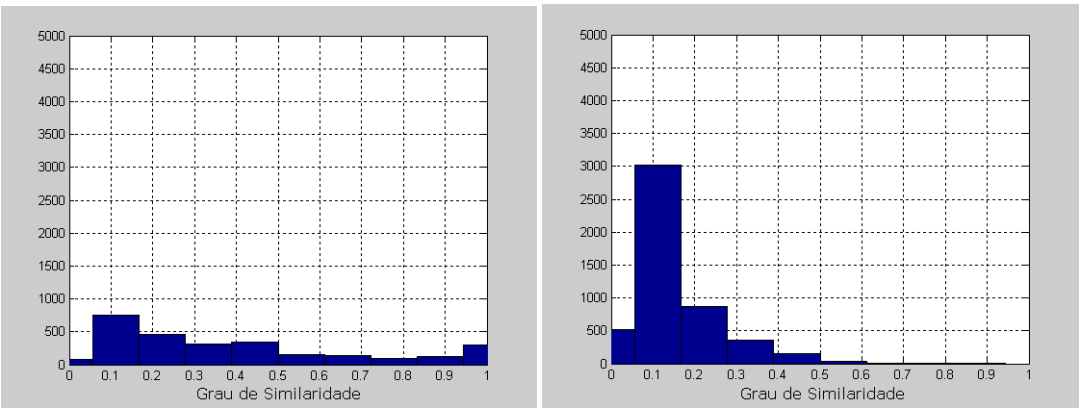


Figura F.4: Curva FAR(t) e Curva FRR(t) do Banco DB3 FVC/2000

Tabela F.3: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB4 FVC/2000

TESTE_CAR.LOCAIS_2000DB4			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.41	6.53	0.10s
Mediana	0.33	5.00	0.06s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	28.00	1.19s
Desvio Padrão	0.30	4.57	0.12s
	Reconhecimento Impostor		
Média	0.16	3.01	0.08s
Mediana	0.17	3.00	0.06s
Mínimo	0.00	1.00	0.01s
Máximo	0.92	12.00	1.47s
Desvio Padrão	0.11	1.39	0.08s
$REJ_{veri} = 0$	$EER = 0.29$	$ZeroFAR = 0.88$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.5: Histogramas do Grau de Similaridade do Banco DB4 FVC/2000

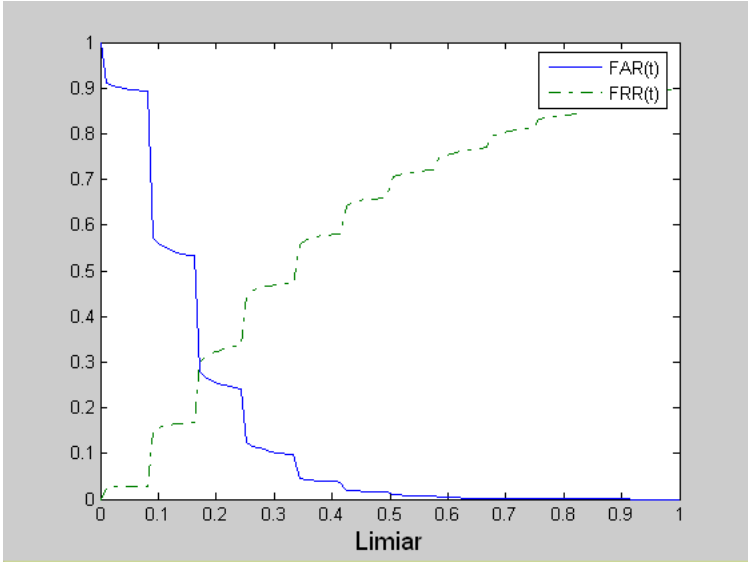
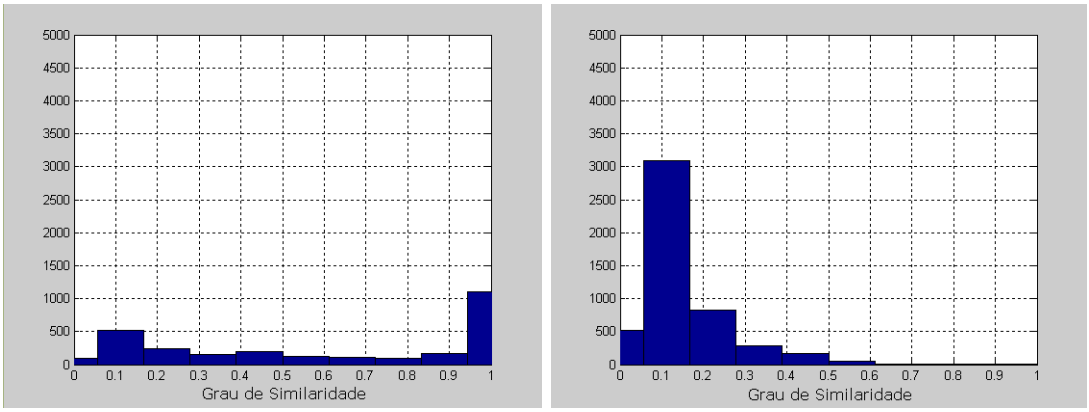


Figura F.6: Curva FAR(t) e Curva FRR(t) do Banco DB4 FVC/2000

Tabela F.4: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB1 FVC/2002

TESTE_CAR.LOCAIS_2002DB1			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.62	11.42	0.16s
Mediana	0.67	10.00	0.11s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	52.00	1.94s
Desvio Padrão	0.37	8.62	0.17s
	Reconhecimento Impostor		
Média	0.16	3.00	0.11s
Mediana	0.17	3.00	0.08s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	14.00	0.92s
Desvio Padrão	0.11	1.40	0.08s
$REJ_{veri} = 0$	$EER = 0.24$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.7: Histogramas do Grau de Similaridade do Banco DB1 FVC/2002

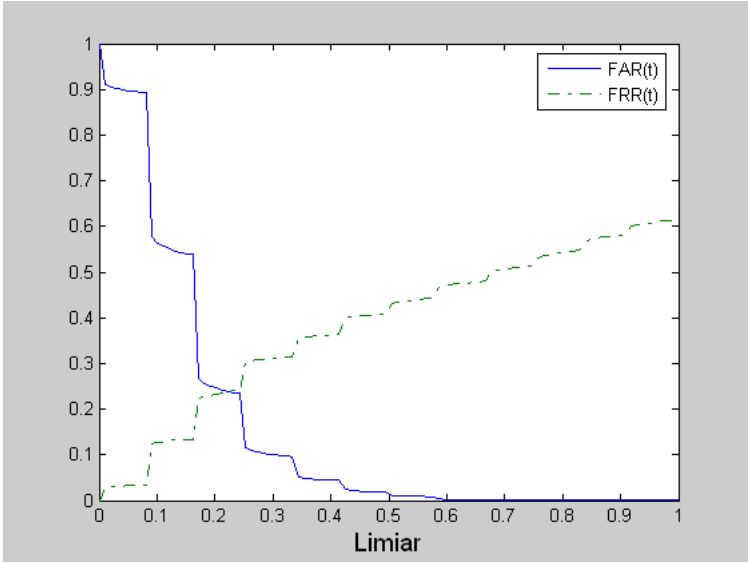
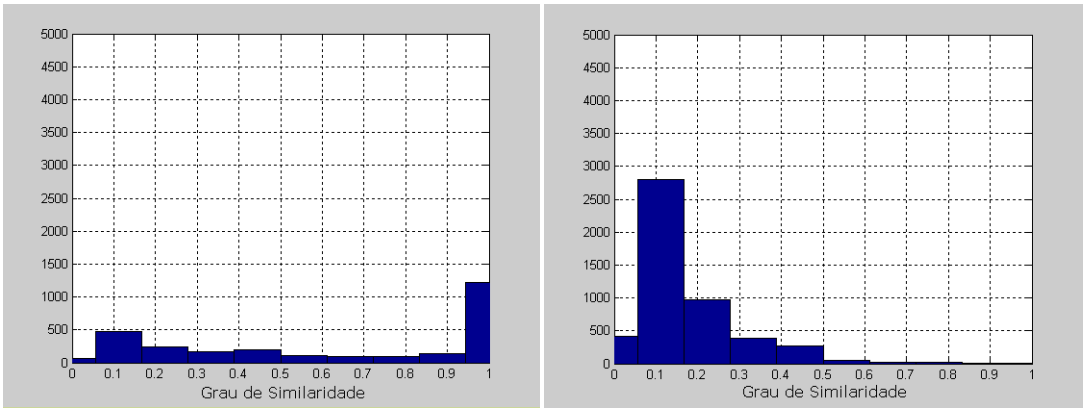


Figura F.8: Curva FAR(t) e Curva FRR(t) do Banco DB1 FVC/2002



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.9: Histogramas do Grau de Similaridade do Banco DB2 FVC/2002

Tabela F.5: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB2 FVC/2002

TESTE_CAR.LOCAIS_2002DB2			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.64	12.80	0.56s
Mediana	0.75	10.00	0.41s
Mínimo	0.00	1.00	0.02s
Máximo	1.00	59.00	16.17s
Desvio Padrão	0.37	10.02	0.80s
	Reconhecimento Impostor		
Média	0.18	3.28	0.45s
Mediana	0.17	3.00	0.33s
Mínimo	0.00	1.00	0.03s
Máximo	1.00	13.00	4.05s
Desvio Padrão	0.13	1.60	0.42s
$REJ_{veri} = 0$	$EER = 0.22$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$

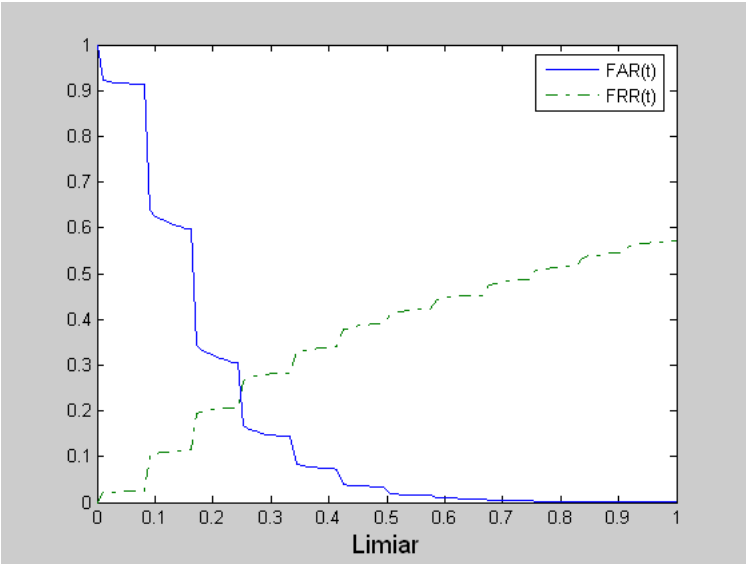
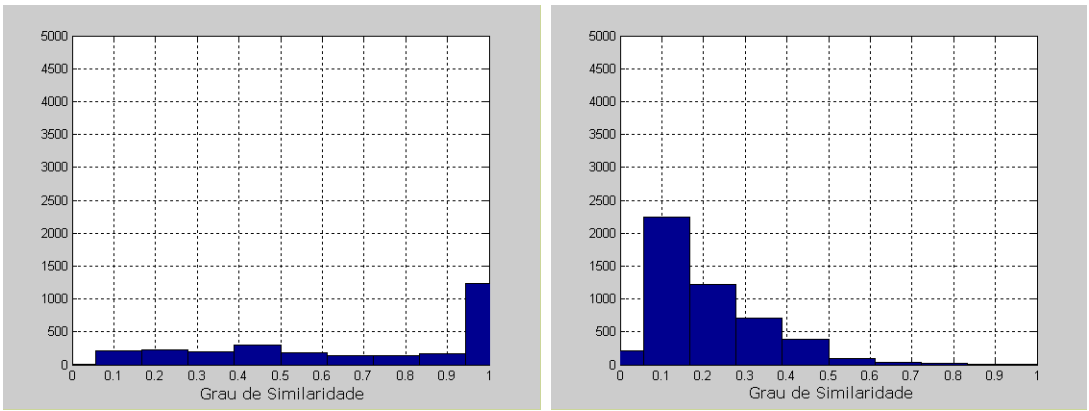


Figura F.10: Curva FAR(t) e Curva FRR(t) do Banco DB2 FVC/2002

Tabela F.6: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB3 FVC/2002

TESTE_CAR.LOCAIS_2002DB3			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.70	14.02	9.14s
Mediana	0.82	11.00	0.97s
Mínimo	0.00	1.00	0.05s
Máximo	1.00	64.00	562.09s
Desvio Padrão	0.32	10.08	39.24s
	Reconhecimento Impostor		
Média	0.22	3.83	2.01s
Mediana	0.17	4.00	0.94s
Mínimo	0.00	1.00	0.06s
Máximo	1.00	15.00	79.33s
Desvio Padrão	0.14	1.75	3.78s
$REJ_{veri} = 0.062$	$EER = 0.17$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.11: Histogramas do Grau de Similaridade do Banco DB3 FVC/2002

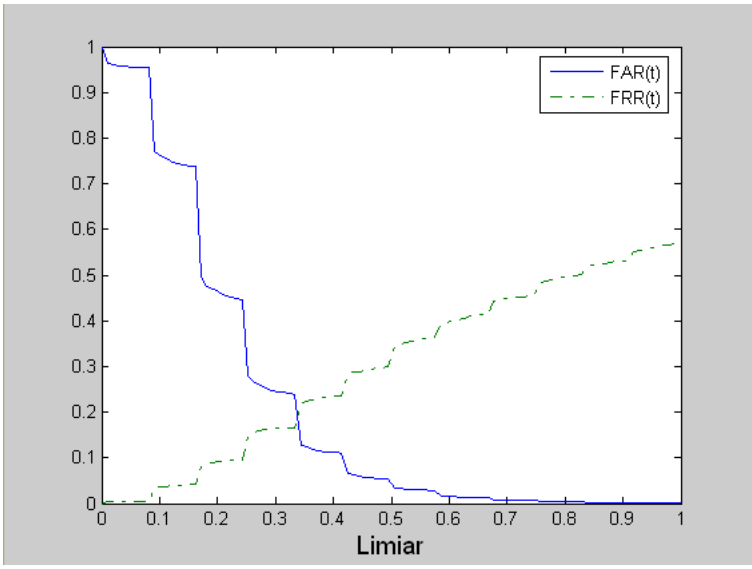
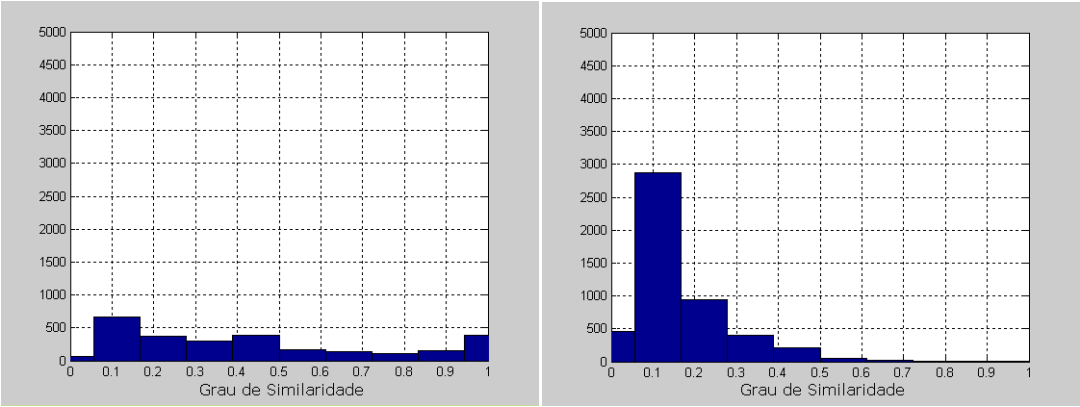


Figura F.12: Curva FAR(t) e Curva FRR(t) do Banco DB3 FVC/2002

Tabela F.7: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB* FVC*

TESTE_CAR.LOCAIS_2002DB4			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.45	7.24	0.10s
Mediana	0.36	6.00	0.06s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	32.00	3.06s
Desvio Padrão	0.31	5.11	0.19s
	Reconhecimento Impostor		
Média	0.17	3.17	0.13s
Mediana	0.17	3.00	0.08s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	16.00	2.22s
Desvio Padrão	0.12	1.53	0.15s
$REJ_{veri} = 0$	$EER = 0.29$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.13: Histogramas do Grau de Similaridade do Banco DB4 FVC/2002

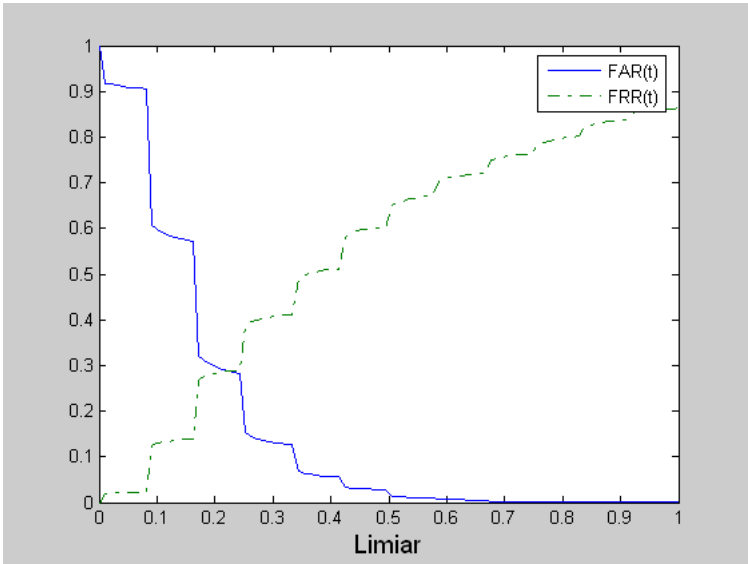
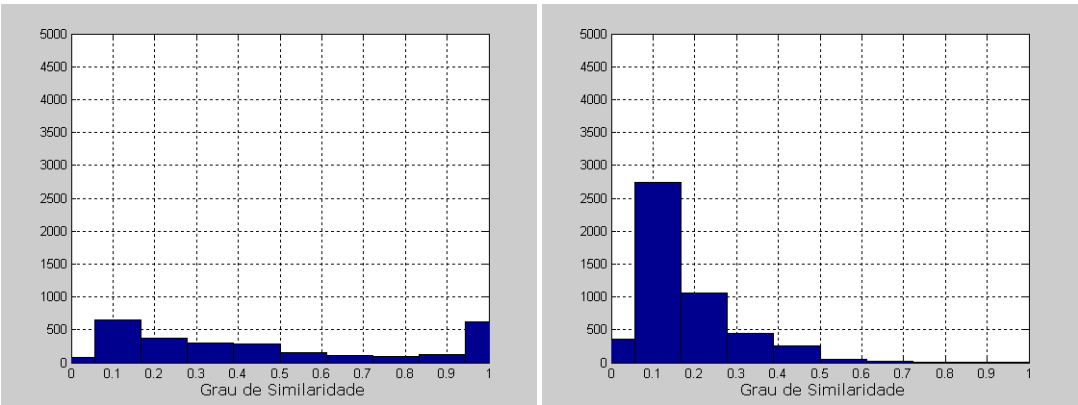


Figura F.14: Curva FAR(t) e Curva FRR(t) do Banco DB4 FVC/2002

Tabela F.8: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB1 FVC/2004

TESTE_CAR.LOCAIS_2004DB1			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.49	8.50	0.43s
Mediana	0.39	6.00	0.25s
Mínimo	0.00	1.00	0.01s
Máximo	1.00	42.00	11.28s
Desvio Padrão	0.34	6.86	0.62s
	Reconhecimento Impostor		
Média	0.18	3.32	0.25s
Mediana	0.17	3.00	0.20s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	17.00	1.59s
Desvio Padrão	0.12	1.57	0.18s
$REJ_{veri} = 0$	$EER = 0.28$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.15: Histogramas do Grau de Similaridade do Banco DB1 FVC/2004

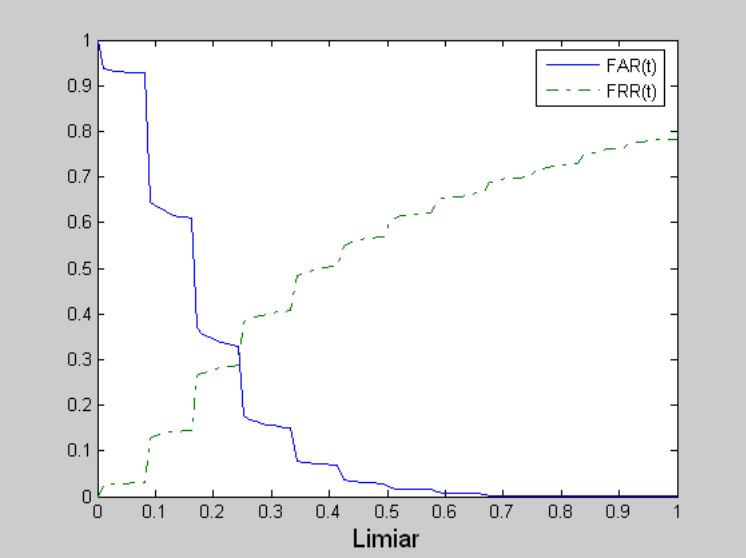
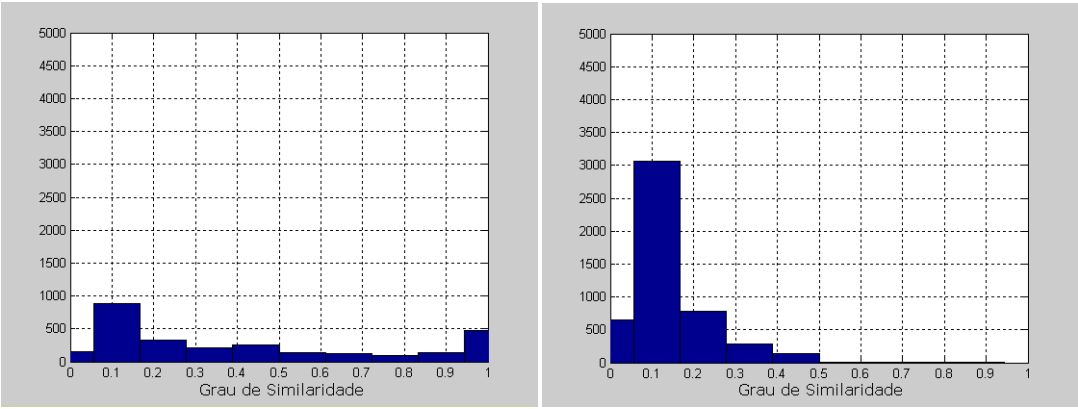


Figura F.16: Curva FAR(t) e Curva FRR(t) do Banco DB1 FVC/2004

Tabela F.9: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB2 FVC/2004

TESTE_CAR.LOCAIS_2004DB2			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.43	7.09	0.12s
Mediana	0.31	5.00	0.06s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	38.00	5.77s
Desvio Padrão	0.34	5.82	0.23s
	Reconhecimento Impostor		
Média	0.14	2.85	0.08s
Mediana	0.10	3.00	0.06s
Mínimo	0.00	1.00	0.00s
Máximo	0.83	11.00	1.67s
Desvio Padrão	0.11	1.34	0.08s
$REJ_{veri} = 0$	$EER = 0.31$	$ZeroFAR = 0.80$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.17: Histogramas do Grau de Similaridade do Banco DB2 FVC/2004

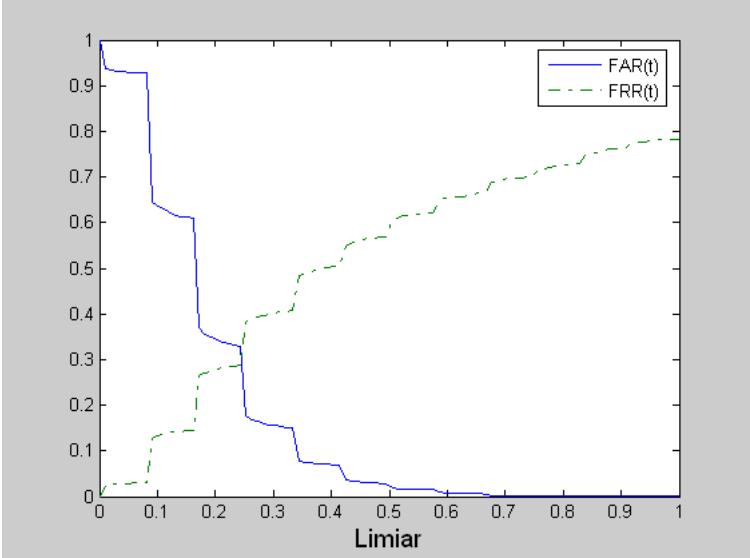
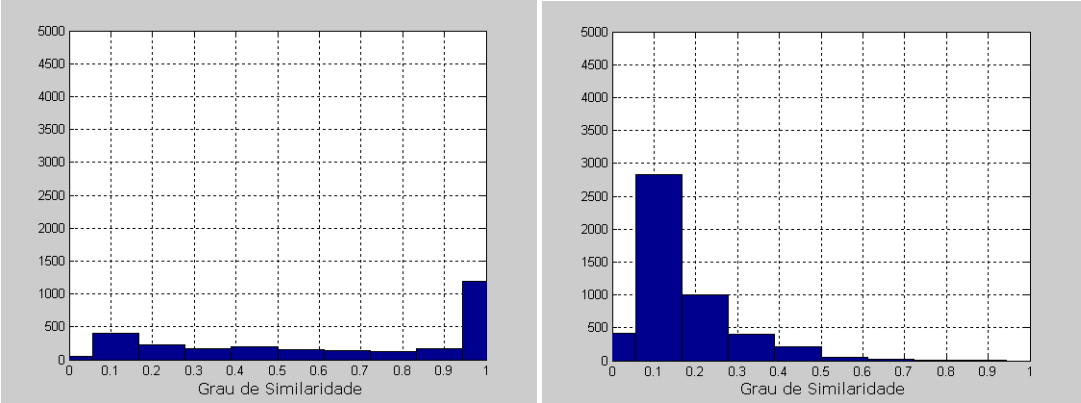


Figura F.18: Curva FAR(t) e Curva FRR(t) do Banco DB2 FVC/2004



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.19: Histogramas do Grau de Similaridade do Banco DB3 FVC/2004

Tabela F.10: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB3 FVC/2004

TESTE_CAR.LOCAIS_2004DB3			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.66	12.04	0.59s
Mediana	0.76	11.00	0.45s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	51.00	9.20s
Desvio Padrão	2.5	8.26	0.70s
	Reconhecimento Impostor		
Média	0.17	3.21	0.41s
Mediana	0.17	3.00	0.33s
Mínimo	0.00	1.00	0.03s
Máximo	0.87	13.00	2.61s
Desvio Padrão	0.12	1.50	0.33s
$REJ_{veri} = 0$	$EER = 0.19$	$ZeroFAR = 0.54$	$ZeroFRR = 1.00$

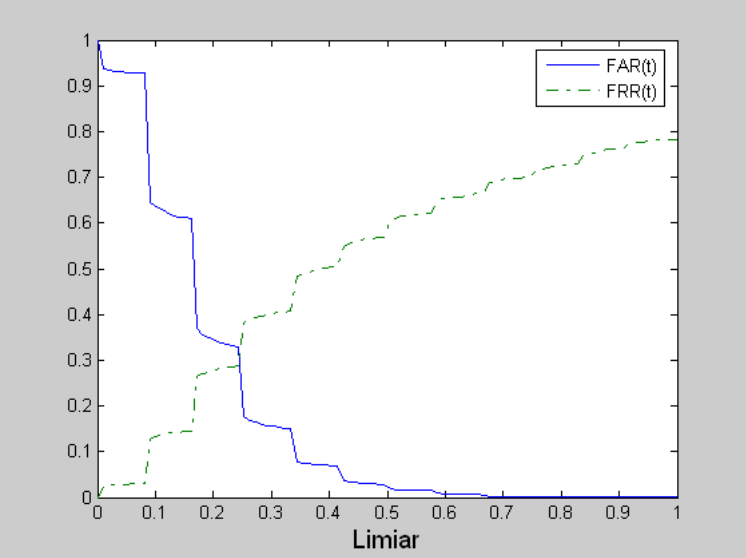
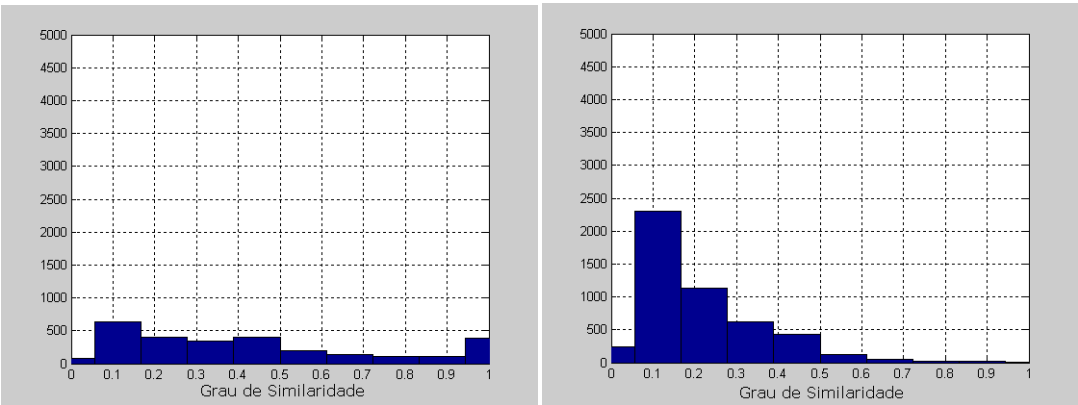


Figura F.20: Curva FAR(t) e Curva FRR(t) do Banco DB3 FVC/2004

Tabela F.11: Resultados sobre o Processo de Verificação utilizando o Método Características Locais com o Parâmetros $n = 12$, $\Delta s = 30$ e $\Delta\theta = 30$ para o Banco DB4 FVC/2004

TESTE_CAR.LOCAIS_2004DB4			
	Grau de Similaridade	Número Minúcias Equivalente	Tempo de Verificação
	Reconhecimento Genuíno		
Média	0.44	7.31	0.25s
Mediana	0.34	6.00	0.17s
Mínimo	0.00	1.00	0.00s
Máximo	1.00	37.00	3.32s
Desvio Padrão	0.30	5.56	0.27s
	Reconhecimento Impostor		
Média	0.22	3.82	0.25s
Mediana	0.17	3.00	0.17s
Mínimo	0.00	1.00	0.02s
Máximo	1.00	15.00	2.30s
Desvio Padrão	0.15	1.84	0.24s
$REJ_{veri} = 0$	$EER = 0.33$	$ZeroFAR = 1.00$	$ZeroFRR = 1.00$



(a) Distribuição Genuíno (b) Distribuição Impostor

Figura F.21: Histogramas do Grau de Similaridade do Banco DB4 FVC/2004

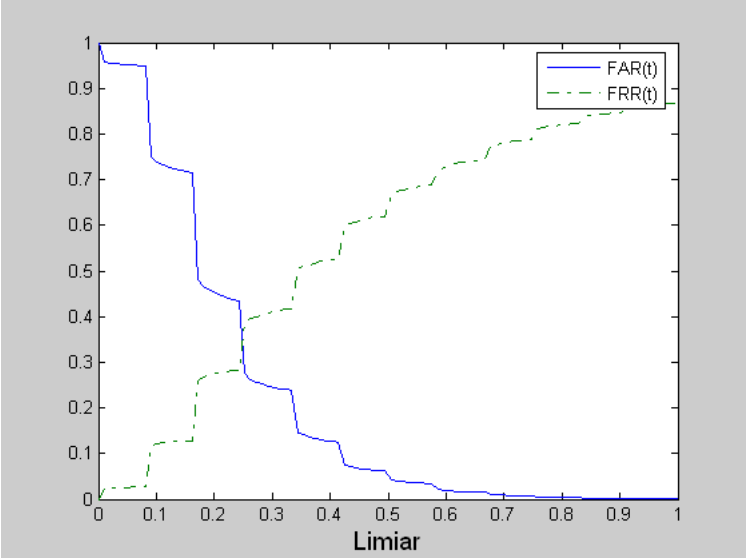


Figura F.22: Curva FAR(t) e Curva FRR(t) do Banco DB4 FVC/2004