

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**TÉCNICAS DE PROCESSAMENTO DE IMPRESSÕES
DIGITAIS PARA CRIAÇÃO DE BANCO DE MINÚCIAS DE
ALTA QUALIDADE**

MATEUS CAMPOS PUTTINI

ORIENTADOR: RICARDO STACIARINI PUTTINI

DISSERTAÇÃO DE MESTRADO

PUBLICAÇÃO: 335/08

BRASÍLIA / DF: 3/2008

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**TÉCNICAS DE PROCESSAMENTO DE IMPRESSÕES
DIGITAIS PARA CRIAÇÃO DE BANCO DE MINÚCIAS DE
ALTA QUALIDADE**

MATEUS CAMPOS PUTTINI

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

**RICARDO STACIARINI PUTTINI, Doutor, ENE-UnB
(ORIENTADOR)**

**ANDERSON NASCIMENTO, Doutor, ENE-UnB
(EXAMINADOR INTERNO)**

**MAMEDE LIMA-MARQUES, Doutor, CID-UnB
(EXAMINADOR EXTERNO)**

**RAFAEL TIMÓTEO DE SOUSA JR., Doutor, ENE-UnB
(SUPLENTE)**

DATA: BRASÍLIA/DF, 12 DE MARÇO DE 2008.

FICHA CATALOGRÁFICA

FERNANDES, MATEUS CAMPOS PUTTINI. Técnicas de processamento de impressões digitais para criação de banco de minúcias de alta qualidade [Distrito Federal] 2008, (83)p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2008).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Impressão digital 2. Extração de minúcias
3. Identificação biométrica

I. ENE/FT/UnB. II. Título (Série)

CESSÃO DE DIREITOS

NOME DO AUTOR: Mateus Campos Puttini Fernandes

TÍTULO DA DISSERTAÇÃO: Técnicas de processamento de impressões digitais para criação de banco de minúcias de alta qualidade.

GRAU/ANO: Mestre/2008.

É concedida à Universidade de Brasília permissão para reproduzir cópias desta Dissertação de Mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte desta dissertação de mestrado pode ser reproduzida sem a autorização por escrito do autor.

Mateus Campos Puttini Fernandes
SHIN QI 12 Conjunto 05 Casa 17
CEP 71525-250 – Lago Norte – DF – Brasil

AGRADECIMENTOS

À minha esposa, Soninha, pelo apoio incondicional e por todo o carinho com que cuidou de mim durante esse trabalho. Minha fonte de inspiração e força não poderia ser outra.

À minha mãe, Ceissa, pela paciência e disposição com que sempre me acolheu e ajudou. Sou quem sou pelo amor com que ela me nutriu.

Ao meu pai, Caetano, pelo imenso suporte e incentivo dado durante todo o tempo em que estive envolvido em mais esta jornada de estudos e pela total confiança em que eu pudesse chegar até o fim de mais essa etapa.

Aos meus sogros, Dorinha e Manoel, pela referência de determinação e disciplina.

Aos meus amigos e irmãos que me incentivaram durante todos esses anos.

À minha família, e a todos que sempre me apoiaram.

A todos, os meus sinceros agradecimentos.

Mateus Campos Puttini Fernandes

À minha amada, Soninha.

RESUMO

Este trabalho propõe uma técnica para o cadastro de impressões digitais e a criação de um banco de dados biométricos de alta qualidade que possa ser utilizado por uma aplicação desse tipo. Uma pesquisa bibliográfica foi realizada para levantar o estado da arte nesta área. A técnica proposta é formada por uma seqüência de processamentos, podendo cada um ser realizado por meio de técnicas específicas. Para algumas das técnicas de processamento selecionadas foram propostas melhorias, sendo elas: a extração de poros, a definição da área útil, o afinamento, a filtragem das minúcias falsas. Uma aplicação de teste foi criada para processar um banco bem conhecido de impressões digitais, o DB1 da FVC2004. Os resultados foram analisados por meio da porcentagem de minúcias verdadeiras contidas no banco de dados biométricos gerado. A qualidade final do banco de dados obtido é boa, mas alguns trabalhos futuros são apontados para aumentar a qualidade final dos resultados.

ABSTRACT

This work proposes a technique for the enrollment of fingerprints and the creation of a high quality biometric data base that can be used by an application of this type. A research was carried through to raise the state of the art in this area. The proposed technique is constituted by a sequence of several processing steps, each one being carried through by means of specific techniques. Improvements were proposed for some of the selected processing techniques, such as: the pore extraction, the definition of the image useful area, the thinning and the filtering of the false minutiae. A test application was created to process a well known bank of fingerprints, the DB1 of the FVC2004. The results have been analyzed by means of the percentage of true minutiae contained in the biometric data base generated. The quality of the obtained data base is good, but some future works are pointed out to increase the final quality of the results.

ÍNDICE

1. Introdução	14
2. Biometria De Impressões Digitais	20
2.1. Minúcias	20
2.2. Processo de identificação biométrica	22
2.2.1. Cadastro	22
2.2.1.1. Coleta da impressão digital	23
2.2.1.2. Extração das minúcias	25
2.2.1.3. Criação do template	33
2.2.2. Identificação	38
3. Padrões Internacionais Considerados	41
3.1. ISO/IEC 19794-2	41
3.1. BioAPI	45
4. Implementações e Testes	48
4.1. Extração de poros	52
4.1.1. Procedimento de teste	57
4.1.2. Análise dos resultados	59
4.2. Definição da área útil	60
4.2.1. Procedimento de teste	64
4.2.2. Análise dos resultados	65
4.3. Afinamento	66
4.3.1. Procedimento de teste	70
4.3.2. Análise dos resultados	71
4.4. Localização e filtragem das minúcias	71
4.4.1. Procedimento de teste	76
4.4.2. Análise dos resultados	78
4.5. Análise geral dos resultados	78
5. Conclusão	80
6. Referências Bibliográficas	83
Anexo A – Transformada de Hough [42]	87
Anexo B – Cálculo do Mapa de Frequências [7]	89

ÍNDICE DE TABELAS

TABELA 2.1 – RESUMO DO FORMATO DO REGISTRO DE MINÚCIAS (FONTE: [11] TRADUZIDA)...	42
TABELA 2.2 – CÓDIGOS DAS POSIÇÕES DOS DEDOS.....	43
TABELA 2.3 – CÓDIGOS DOS TIPOS DE IMPRESSÕES.	43
TABELA 2.4 – CÓDIGOS DE TIPOS DE DADOS ESTENDIDOS	43
TABELA 2.5 – PROPOSTA DE FORMATO PARA A CLASSE DA VISÃO DE DEDO.	44
TABELA 4.1 – MEDIDAS OBTIDAS PELA CONTAGEM DE POROS FALSOS.....	58
TABELA 4.2 – MEDIDAS RELACIONANDO DIMENSÃO DO MODELO DE PORO E NÚMERO DE MINÚCIAS FALSAS ENCONTRADAS AO FINAL DO PROCESSAMENTO.	59
TABELA 4.3 – RESULTADOS OBTIDOS COM A UTILIZAÇÃO DAS TÉCNICAS DE DEFINIÇÃO DA ÁREA ÚTIL.....	65
TABELA 4.4 – RESULTADOS OBTIDOS APÓS O PROCESSO DE AFINAMENTO.	71
TABELA 4.5 – RESULTADOS DA FILTRAGEM DE MINÚCIAS.....	77

ÍNDICE DE FIGURAS

FIGURA 2.1 – MINÚCIAS. A) TERMINAÇÃO B) BIFURCAÇÃO	21
FIGURA 2.2 – PONTOS CARACTERÍSTICOS (FONTE: [17]).....	21
FIGURA 2.3 – PROCESSO BÁSICO DE UM SISTEMA DE IDENTIFICAÇÃO DE IMPRESSÕES DIGITAIS.	22
FIGURA 2.4 – IMPRESSÕES DIGITAIS: A) ROLADA B) POUSADA. IMAGENS EXTRAÍDAS DO MESMO DEDO.	24
FIGURA 2.5 – IMPRESSÕES DIGITAIS CAPTURADAS POR DIFERENTES DE SENSORES. DA ESQUERDA PARA A DIREITA E DE CIMA PARA BAIXO: SENSOR ÓTICO “V300” DA MARCA CROSSMATCH, SENSOR ÓTICO “U.ARE.U 4000” DA MARCA DIGITAL PERSONA, SENSOR DE VARREDURA TÉRMICA DA MARCA "FINGERCHIP FCD4B14CB" DA ATMEL E IMPRESSÃO DIGITAL GERADA ARTIFICIALMENTE PELO SOFTWARE SFINGE v3.0 [21].	25
FIGURA 2.6 – FILTRO DE MÉDIA MÓVEL APLICADO A UMA IMPRESSÃO DIGITAL. A) IMAGEM ORIGINAL E B) RESULTADO DA FILTRAGEM.	28
FIGURA 2.7 - IMPRESSÃO DIGITAL ORIGINAL E SEU CAMPO DIRECIONAL.	29
FIGURA 2.8 – MÁSCARAS DE DEFINIÇÃO DA ÁREA ÚTIL. A) DESVIO PADRÃO B) FREQUÊNCIA C) UNIÃO DAS DUAS TÉCNICAS.	29
FIGURA 2.9 – PRÉ-PROCESSAMENTO. A) IMPRESSÃO DIGITAL ORIGINAL B) RESULTADO DA EXTRAÇÃO DE POROS C) RESULTADO DA SUAVIZAÇÃO D) MÁSCARA QUE DEFINE A ÁREA ÚTIL E) RESULTADO DA FILTRAGEM PELO FILTRO DE GABOR.....	30
FIGURA 2.10 – BINARIZAÇÃO. A) IMAGEM RESULTANTE DO PRÉ-PROCESSAMENTO B) IMAGEM BINARIZADA.	31
FIGURA 2.11 – IMPRESSÃO DIGITAL AFINADA.....	31
FIGURA 2.12 – EXTRAÇÃO DE MINÚCIAS. A) IMAGEM AFINADA B) MINÚCIAS EXTRAÍDAS POR INSPEÇÃO DAS LINHAS C) MINÚCIAS QUE PASSARAM PELO FILTRO DE MINÚCIAS ESPÚRIAS	32

FIGURA 2.13 – PROCESSO DE UTILIZAÇÃO DE MÚLTIPLAS IMPRESSÕES DIGITAIS PARA REALIZAR O CADASTRO DO <i>TEMPLATE</i> (FONTE: [20]).	34
FIGURA 2.14 – EXEMPLOS DE IMPRESSÕES DIGITAIS PERTENCENTES ÀS CLASSES CONSIDERADAS PELA TÉCNICA UTILIZADA. DA ESQUERDA PARA A DIREITA, NA PRIMEIRA LINHA: NINHO, ARCO E LAÇO ESQUERDO; NA SEGUNDA LINHA: ARCO APOIADO E LAÇO DIREITO.	35
FIGURA 2.15 – MÁSCARAS DINÂMICAS DO ALGORITMO DE CLASSIFICAÇÃO. DA ESQUERDA PARA A DIREITA, DE CIMA PARA BAIXO: NINHO, LAÇO ESQUERDO, ARCO, ARCO APOIADO E LAÇO DIREITO.	36
FIGURA 2.16 – EXEMPLO DE ADAPTAÇÃO DE MÁSCARA DINÂMICA A UMA IMPRESSÃO DIGITAL DA CLASSE LAÇO ESQUERDO (FONTE: [31]).	37
FIGURA 2.17 – EMPARELHAMENTO DE MINÚCIAS (FONTE: [33] COM ALTERAÇÕES).	39
FIGURA 2.18 – ESTRUTURA DE UMA APLICAÇÃO DE BIOMETRIA (FONTE: [12])	46
FIGURA 4.1 – DETALHAMENTO DAS OPERAÇÕES REALIZADAS PARA O PROCESSAMENTO DA IMAGEM DA IMPRESSÃO DIGITAL COLETADA.	48
FIGURA 4.2 – OPERAÇÕES REALIZADAS PARA O CADASTRO DE UMA IMPRESSÃO DIGITAL. AS IMAGENS ILUSTRAM OS SEGUINTE PROCESSOS: A) IMAGEM ORIGINAL CAPTURADA, B) EXTRAÇÃO DE POROS, C) SUAVIZAÇÃO POR FILTRO DE MÉDIA MÓVEL, D) CÁLCULO DO CAMPO DIRECIONAL, E) DEFINIÇÃO DA ÁREA ÚTIL (MÁSCARA), F) FILTRAGEM DE GABOR, G) BINARIZAÇÃO, H) AFINAMENTO, I) EXTRAÇÃO DAS MINÚCIAS E J) FILTRAGEM DE MINÚCIAS FALSAS.	49
FIGURA 4.3 – EXEMPLOS DE IMAGENS CONTIDAS NO BANCO DE IMPRESSÕES DIGITAIS DB1 DA FVC2004. À ESQUERDA, DUAS IMAGENS DE BOA QUALIDADE; AO CENTRO, DUAS DE QUALIDADE REGULAR; E À DIREITA, DUAS DE MÁ QUALIDADE.	51
FIGURA 4.4 – MODELO UTILIZADO PARA OS POROS DA PELE QUE APARECEM NA IMPRESSÃO DIGITAL.	53
FIGURA 4.5 – PROPOSTA DE PREENCHIMENTO DO PORO – CONSIDERANDO O MAIOR NÍVEL DE CINZA DA IMAGEM DA IMPRESSÃO DIGITAL ORIGINAL COMO SENDO 255.	55

FIGURA 4.6 – PROCESSO DE IDENTIFICAÇÃO E EXTRAÇÃO DE POROS. DA ESQUERDA PARA A DIREITA, DE CIMA PARA BAIXO: IMAGEM ORIGINAL, MAPA DOS ERROS QUADRÁTICOS, PREENCHIMENTO PARA OS POROS DETECTADOS, IMAGEM COM OS POROS COBERTOS.	56
FIGURA 4.7 – TÉCNICA UTILIZADA PARA CONTAGEM DE POROS FALSOS. NA AMPLIAÇÃO, OS POROS APONTADOS SÃO CONSIDERADOS FALSOS.	58
FIGURA 4.8 – IMAGEM AFINADA SEM A EXTRAÇÃO DE POROS (ESQUERDA) E COM A EXTRAÇÃO DE POROS (DIREITA).....	59
FIGURA 4.9 – MÁSCARA DE ÁREA ÚTIL DEFINIDA POR DESVIO PADRÃO DOS NÍVEIS DE CINZA. A) IMAGEM ORIGINAL. MÁSCARAS OBTIDAS PELA INSPEÇÃO DA IMPRESSÃO DIGITAL: B) DA ESQUERDA PARA A DIREITA E DE CIMA PARA BAIXO, C) DA DIREITA PARA A ESQUERDA E DE CIMA PARA BAIXO, D) DA ESQUERDA PARA A DIREITA E DE BAIXO PARA CIMA, E) DA DIREITA PARA A ESQUERDA E DE BAIXO PARA CIMA. F) MÁSCARA FINAL.	62
FIGURA 4.10 – TÉCNICA DE DEFINIÇÃO DA ÁREA ÚTIL ATRAVÉS DO MAPA FREQUENCIAL. A) IMAGEM DA IMPRESSÃO DIGITAL, B) RESULTADO DA INSPEÇÃO DO MAPA DE FREQUÊNCIAS, C) DILATAÇÃO DA ÁREA ÚTIL, E D) EROÇÃO DA ÁREA ÚTIL.	63
FIGURA 4.11 – UNIÃO DAS DUAS TÉCNICAS DE DEFINIÇÃO DA ÁREA ÚTIL. DA ESQUERDA PARA A DIREITA: TÉCNICA DE LIMIAR DO DESVIO PADRÃO DOS NÍVEIS DE CINZA, TÉCNICA DE INSPEÇÃO DO MAPA DE FREQUÊNCIAS E SOBREPOSIÇÃO DO RESULTADO DAS DUAS TÉCNICAS.	64
FIGURA 4.12 – DIAGRAMA PARA ANÁLISE DO RESULTADO DA TABELA 4.3.....	65
FIGURA 4.13 – MODELOS DE SUAVIZAÇÃO (FONTE: [8]).....	68
FIGURA 4.14 – A) NOTAÇÃO UTILIZADA PARA O PIXEL A SER ANALISADO, P_0 , E SUA VIZINHANÇA, P_1 A P_8 . B) NOTAÇÃO UTILIZADA PARA REPRESENTAR O MAPA DE MARCAÇÕES REFERENTE A P_0	68
FIGURA 4.15 – MODELOS DE SUAVIZAÇÃO PROPOSTOS POR ESTE TRABALHO.....	70

FIGURA 4.16 – EXEMPLO DE UTILIZAÇÃO DE MODELO DE SUAVIZAÇÃO. A) VÁRIOS PONTOS CLASSIFICÁVEIS COMO BIFURCAÇÃO – VER SEÇÃO 4.4; B) MÚLTIPLAS MINÚCIAS ELIMINADAS PELA UTILIZAÇÃO DO MODELO DE SUAVIZAÇÃO DA FIGURA 4.15I.	70
FIGURA 4.17 – EXEMPLOS DE PONTOS ANALISADOS PARA A LOCALIZAÇÃO DE MINÚCIAS. A) 1 VIZINHO, MINÚCIA DE TERMINAÇÃO B) DOIS VIZINHOS, AUSÊNCIA DE DESCONTINUIDADE C) 3 VIZINHOS, MINÚCIA DE BIFURCAÇÃO	72
FIGURA 4.18 – EXEMPLOS DE ESTRUTURAS QUE APRESENTAM FALSAS MINÚCIAS (FONTE: [9] COM ADAPTAÇÕES).....	73
FIGURA 4.19 – SEQÜÊNCIA DE PASSOS DO ALGORITMO DE DETECÇÃO DE FALSAS MINÚCIAS. ...	75
FIGURA 4.20 – SEQÜÊNCIA DE PASSOS REALIZADOS PARA DETECTAR UMA MINÚCIA DO TIPO BIFURCAÇÃO FALSA.....	75
FIGURA 4.21 – TÉCNICA UTILIZADA PARA CONTAGEM DAS MINÚCIAS FALSAS OBTIDAS AO FINAL DE TODO O PROCESSAMENTO: SOBREPOSIÇÃO DA IMAGEM ORIGINAL COM AS MINÚCIAS ENCONTRADAS. AS MINÚCIAS CIRCULADAS SÃO CONSIDERADAS FALSAS.	77

1. INTRODUÇÃO

A biometria tem-se tornado uma das mais efetivas ferramentas de identificação em sistemas de informação [1]. Utiliza-se a identificação biométrica para controlar o acesso a computadores pessoais, a ambientes físicos restritos, a redes de comunicação, entre outros. Biometria, em seu significado comumente aceito, é a ciência que estuda a mensuração dos seres vivos. Na área de tecnologia da informação, a palavra biometria está ligada à verificação da identidade de uma pessoa por meio de uma característica física única, característica essa que pode ser desde uma impressão digital, passando por imagem de íris, amostragem de voz, caligrafia e projeção facial, até diferenciação postural verificada pela pressão dos pés ao caminhar.

Os sistemas de identificação humana que utilizam medidas biométricas para identificar os indivíduos têm-se tornado cada vez mais difundidos. Muitas aplicações atuais utilizam a biometria como meio de identificação de seus usuários. Os dados biométricos são associados a dados pessoais dos usuários para acrescentar segurança aos processos de identificação e controle de acesso, tanto para aplicações de software quanto para ambientes físicos restritos. As identificações biométricas, por não serem facilmente substituídas, falsificadas ou compartilhadas, são consideradas mais complexas de serem fraudadas do que *tokens* tradicionais (p.ex. chaves) ou segredos (p.ex. senhas) [1]. Assim, quando associada a outras técnicas de segurança, a biometria pode ser utilizada para aumentar o nível de segurança de informação.

O tipo de biometria mais utilizado atualmente é o de impressões digitais [1]. As impressões digitais apresentam muitas características que favorecem sua utilização em aplicações de identificação biométrica que requerem um bom nível de segurança, velocidade de processamento, facilidade de coleta de amostras e baixo custo. Algumas dessas características são: o fato de a impressão digital de um indivíduo não se alterar com a idade (alguns efeitos de desgaste da superfície dos dedos podem ocorrer, mas os pontos particulares continuam apresentando a mesma configuração); a unicidade da impressão digital por indivíduo (até mesmo indivíduos gêmeos univitelinos apresentam impressões digitais totalmente distintas); o fato de imagens em graus de cinza relativamente simples serem suficientes como amostra da impressão digital para utilização em sistemas de identificação automáticos; as dimensões e o preço dos leitores

de impressões digitais modernos, permitindo que sejam acoplados até mesmo a aparelhos celulares, *mouses* e teclados comuns de computador.

Alguns países já possuem soluções modernas para identificação civil de sua população. Já é relativamente comum que cidadãos de países como Itália, Coreia, Bélgica, Finlândia e outros utilizem aplicações que empregam a identidade civil para garantir segurança aos seus processos. Essas aplicações podem ser sítios do governo que oferecem diversos serviços públicos *on-line*, identificação eleitoral e até serviços jurídicos automatizados que só podem ser prestados com segurança por meio da utilização das técnicas modernas baseadas em identificações civis eletrônicas.

No Brasil a identificação civil é realizada por meio de inúmeros documentos. Registro Geral (RG), Cadastro de Pessoa Física (CPF), título eleitoral, carteira de motorista e carteira de trabalho são apenas alguns exemplos dos diversos documentos utilizados para identificar o cidadão brasileiro. A quantidade de documentos e processos utilizados para identificar o cidadão torna a identificação civil brasileira altamente dispendiosa para o Estado e para o cidadão, além de excessivamente burocrática e confusa para grande parte da população. De fato trata-se de um modelo antiquado de identificação civil.

Esforços já foram realizados na tentativa de melhorar esse modelo, algumas vezes para acrescentar itens de segurança, melhorar a qualidade estética ou usar tecnologia mais moderna em algum documento. Esses esforços, porém, sempre foram um tanto isolados, ou no mínimo fracamente integrados, pois melhoravam um ou outro documento, mas sem questionar nem modificar o modelo em si.

Existe legislação em vigor que estabelece a obrigatoriedade da utilização de um único documento para a identificação civil no Brasil [2]. Essa sim trata de modificação interessante, não só de processos ou documentos isolados, mas do modelo de identificação civil brasileiro como um todo. No entanto, devido à enorme dimensão do País, existe uma infinidade de questões políticas, econômicas, sociais e legais que devem ser levadas em conta para que uma alteração desse porte seja realizada.

Apesar dos obstáculos que ainda impedem a implantação de um novo sistema de identificação civil no Brasil, a Universidade de Brasília – UnB – tomou a iniciativa de propor uma solução tecnológica para o cumprimento da legislação vigente.

Um projeto vem sendo estruturado para atender a esta demanda já legalmente estabelecida. Esse projeto – conhecido por SUI, Sistema Único de Identificação – contempla todos os aspectos tecnológicos necessários à implantação de um modelo de identidade civil única para todo o território brasileiro [3][4].

O Sistema Único de Identificação (SUI) é um sistema informatizado que tem por objetivo apoiar as atividades relacionadas com a identificação da população brasileira, possibilitando a realização de autenticação *on-line* dos cidadãos a partir de técnicas modernas de biometria (impressões digitais). Este sistema pretende atender as necessidades da criação de uma base de dados unificada para armazenamento e controle das informações de identificação do cidadão brasileiro, atendendo às diversas aplicações que necessitem da autenticação segura de sua identidade, dando suporte de maneira flexível e extensível a entidades governamentais e não-governamentais. Em especial, o sistema armazena e organiza informações relevantes para a emissão da carteira de identidade, permitindo uma utilização flexível e interativa dessas informações.

Para autenticação segura dos usuários, propõe-se a utilização de técnicas de biometria voltadas para o reconhecimento de impressões digitais. Essas técnicas vêm possibilitando uma relação custo-benefício satisfatória em experiências de identificação de grandes populações, como, por exemplo, na Coreia.

Um Sistema Automático de Identificação de Impressões Digitais, conhecido na área de identificação biométrica por sua sigla na língua inglesa – AFIS, *Automatic Fingerprint Identification System* – é um dos elementos nucleares do SUI. Este sistema visa a prover as funcionalidades centrais relacionadas à utilização de biometria de impressões digitais para a identificação da população brasileira.

O presente trabalho tem por objetivo propor uma técnica de processamento de impressões digitais para a criação de um banco de dados biométricos de alta qualidade. Para que esse banco de dados possa ser utilizado pelo SUI, as informações biométricas extraídas pela técnica aqui proposta devem ser associadas às informações civis dos cidadãos de forma a compor o banco de identidades do SUI. Contudo essa associação não é foco deste trabalho. Alguns aspectos das informações que acompanham os dados biométricos extraídos das impressões digitais são abordados para contextualizar o desenvolvimento da técnica proposta, como: a observância aos padrões internacionais

pertinentes; a classificação das impressões digitais processadas, a utilização de múltiplas amostras de impressões na criação dos registros de minúcias para aumentar a qualidade do banco. No entanto o foco é no processamento de impressões digitais para extração de minúcias com qualidade.

O AFIS que será utilizado pelo SUI deverá automatizar diversas funcionalidades: o cadastro organizado de impressões digitais associadas às identidades que o SUI gerenciará; o armazenamento dessas impressões digitais em um formato definido por um padrão internacionalmente aceito; a verificação de uma impressão digital – comparação 1:1 (um para um) ou *matching* – e a identificação de uma impressão digital dentre as armazenadas em um banco de dados – comparação 1:n (um para n).

Neste trabalho o foco é na funcionalidade de cadastro. Mais especificamente na extração e formatação de dados biométricos que comporão o cadastro a ser utilizado pelo SUI. Contudo, foram implementados algoritmos básicos para outras funcionalidades – armazenamento e verificação –, com o objetivo auxiliar a validação da técnica proposta e o teste do banco de dados biométricos criado.

Uma pesquisa foi realizada sobre as técnicas mais recentes e mais eficientes relacionadas à biometria de impressões digitais. As informações biométricas de impressões digitais mais utilizadas e pesquisadas atualmente são baseadas nos pontos particulares encontrados nas linhas das impressões digitais, as minúcias [1]. Os tipos de minúcias considerados por este trabalho foram a terminação e a bifurcação de linhas das impressões digitais. Esses tipos são os mais comumente utilizados em sistemas de reconhecimento de impressões digitais baseados em minúcias [1].

Foram selecionadas as técnicas mais interessantes para a construção dos processamentos relativos ao cadastro de identidades em um AFIS. Uma implementação dos algoritmos selecionados foi realizada e testada utilizando-se um banco de dados bem conhecido (DB1 da FVC2004) de amostras de impressões digitais, para que a qualidade das escolhas realizadas fosse validada. Esse banco de impressões digitais é proveniente da FVC2004, competição muito difundida acadêmica e comercialmente, a qual compara sistemas de verificação de impressões digitais [5].

O banco de impressões digitais utilizado foi escolhido por ser aberto e frequentemente referenciado para testes e validações de trabalhos na área de biometria de impressões digitais. Contudo, cabe frisar que este banco contém apenas imagens de impressões digitais e que a única informação acessória a estas imagens é a de qual dedo gerou cada impressão digital.

Foram propostas melhorias para algumas das técnicas de processamento de impressões digitais selecionadas foram propostas melhorias. São estas as técnicas: a extração de poros [6], que tenta eliminar pontos indesejados na imagem da impressão digital coletada, pontos esses que aparecem devido à presença de poros na pele; a definição de área útil [7], que visa a separar as áreas que contêm informação útil na imagem da impressão digital das áreas potencialmente inúteis; o afinamento [8], que trata de estreitar as linhas contidas na impressão digital para facilitar a extração das minúcias; e a filtragem de minúcias falsas [9], que realiza o pós-processamento do conjunto de minúcias extraído para detectar possíveis minúcias espúrias.

As melhorias propostas tiveram, em sua maioria, o objetivo de aumentar a qualidade final do banco de dados biométricos gerado. A maior parte dos trabalhos relacionados a sistemas de identificação que utilizam impressões digitais baseiam a qualificação dos processamentos realizados na fase de *matching*, avaliando porcentagens de falsos positivos, falsos negativos e outros [10]. Contudo, este trabalho é direcionado para a etapa de cadastro e, portanto, esse tipo de avaliação não fornece a visão desejada sobre os resultados da fase de cadastro, mas sim do processo de identificação biométrica como um todo.

Dessa forma, a qualidade do banco de dados biométricos gerado foi avaliada pela porcentagem de informação biométrica verdadeira presente, neste caso, de minúcias. Como o banco de impressões digitais utilizado para os testes (DB1 da FVC2004) não contém informações sobre a localização ou a quantidade das minúcias existentes em cada imagem de impressão digital, a porcentagem de minúcias falsas foi avaliada automaticamente, quando possível, ou pela da contagem visual de minúcias falsas encontradas nas impressões digitais testadas. Alguns trabalhos focados na filtragem de minúcias espúrias (último processamento realizado durante o cadastro) utilizam esta metodologia para avaliar seu resultado [9], mas não foram encontrados

trabalhos que validem dessa forma a fase de cadastro como um todo. Por essa razão procedimentos de teste foram estabelecidos para possibilitar a validação proposta.

A implementação criada, como mencionado, foi projetada para aderir aos padrões internacionais pertinentes, visando a assegurar a reusabilidade. Os padrões selecionados são: a ISO/IEC 19794-2 [11], que trata do formato dos registros de minúcias para comunicação e armazenamento de informações biométricas de impressões digitais, e a BioAPI [12], que define uma interface padronizada para a criação de bibliotecas e aplicações de software que utilizem biometria. Outras contribuições trazidas por este trabalho são a correção de pequenas falhas ou lacunas existentes nas técnicas selecionadas e a diminuição do tempo de processamento gasto para execução de determinada técnica.

Além deste, outros quatro capítulos compõem o presente trabalho. No próximo há uma explanação mais detalhada sobre a biometria de impressões digitais. No terceiro é feita uma descrição sucinta dos padrões internacionais estudados. O seguinte contém a descrição das contribuições e melhorias propostas por este trabalho para o processo de cadastro de impressões digitais acompanhados dos respectivos procedimentos de testes e análises de resultados. As considerações finais e as indicações de trabalhos futuros são apresentadas no capítulo de conclusão.

2. BIOMETRIA DE IMPRESSÕES DIGITAIS

As impressões digitais são formadas por uma série de linhas ou sulcos que se formam na superfície da pele dos dedos. Estas linhas apresentam uma disposição única para cada dedo de cada indivíduo. A unicidade das impressões digitais já é utilizada há centenas de anos como meio de identificar os indivíduos [13][14]. Outra característica interessante das impressões digitais é que a disposição das linhas permanece inalterada com o passar dos anos [1].

Um cadastro confiável é um registro prévio de uma medida biométrica que, geralmente, é associado aos dados que identifiquem um sujeito, fazendo parte, desta forma do registro de identidade do indivíduo. O termo *template*, em inglês, é utilizado para referenciar o cadastro confiável em sistemas de biometria. Uma amostra biométrica cuja autenticidade se pretenda verificar é comumente chamada de *candidata*.

Com base nesses preceitos, inúmeras técnicas podem ser adotadas com o objetivo de verificar automaticamente a autenticidade de uma impressão digital contra um *template*. Podem-se, por exemplo, utilizar os mapas de orientação das linhas da impressão digital [15] visando medir a correlação entre a textura do *template* e a textura da impressão digital *candidata*. Pode-se, ainda, procurar o melhor alinhamento entre as linhas do *template* e da impressão digital *candidata* [16]. A comparação entre dois conjuntos de características para avaliar se ambos representam a mesma impressão digital é freqüentemente chamada *matching*, nome dado a este processo em inglês.

2.1. MINÚCIAS

As linhas de uma impressão digital podem ser caracterizadas pelos vales ou pelos topos, esses máximos e mínimos relativos com relação à superfície do dedo. As linhas de uma impressão digital, independentemente da escolha de vales ou topos para representá-las, podem apresentar dois tipos de interrupções: as terminações e as bifurcações. As terminações são interrupções que criam uma descontinuidade da linha, ou seja, finalizam a linha. As bifurcações dividem a linha em duas, ou, de outra forma, unem duas linhas em uma. Esses pontos particulares, terminações e bifurcações, são conhecidas como minúcias das impressões digitais. A Figura 2.1 mostra um exemplo dos dois tipos de minúcias.

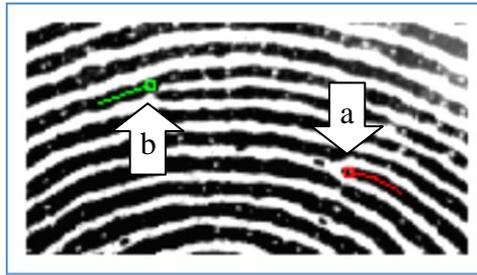


Figura 2.1 – Minúcias. a) terminação b) bifurcação

Uma minúcia se caracteriza pelo tipo – terminação ou bifurcação –, pela posição e pela inclinação – geralmente verificada com relação ao eixo horizontal.

Existem outras características que podem ser utilizadas para auxiliar no processo de comparação entre duas impressões digitais. Uma delas é o número de linhas entre um determinado par de minúcias. Outra é a existência de um ponto característico que pode ser utilizado para facilitar o processo de alinhamento – translacional e rotacional – entre o *template* e a candidata. Este ponto característico pode ser classificado de diversas formas, mas os tipos mais comumente utilizados são o *core* e o *delta*.

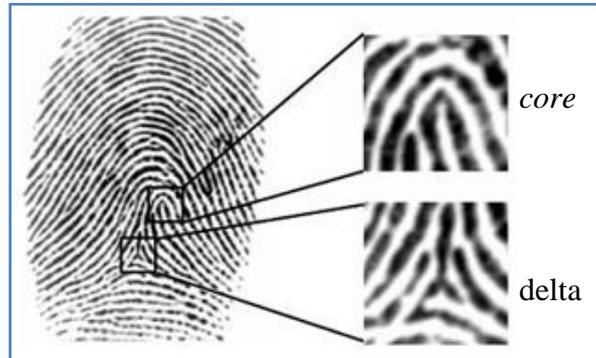


Figura 2.2 – Pontos característicos (fonte: [17]).

O método mais utilizado para comparação entre *template* e candidata é avaliar alguma forma de correlação entre os conjuntos de minúcias extraídos de cada impressão digital. Esta comparação pode ser realizada utilizando diversas técnicas, desde uma simples inspeção minúcia a minúcia até métodos mais robustos que utilizam os pontos característicos para facilitar o processo de comparação [17] ou, ainda, utilizando métodos mais complexos que combinam características pertencentes ao espaço euclidiano – posição e direção, tal como as minúcias – com características baseadas nas

estruturas formadas pelas linhas da impressão digital (número de linhas entre duas minúcias ou formato da linha a que uma minúcia pertence [18]).

2.2. PROCESSO DE IDENTIFICAÇÃO BIOMÉTRICA

Para um sistema de identificação baseado em biometria, independentemente do tipo de biometria utilizado, há uma seqüência bem definida de atividades a serem realizadas para prover, de forma consistente, o serviço de identificação. De forma geral, este processo divide-se em duas fases: o cadastro (em inglês *enrollment*) e a verificação. O cadastro é formado pelas atividades de captura de informações biométricas, extração das características particulares e armazenamento organizado das identidades. A verificação consiste em capturar a amostra biométrica candidata, extrair dela as características particulares e, por fim, realizar o *matching*.

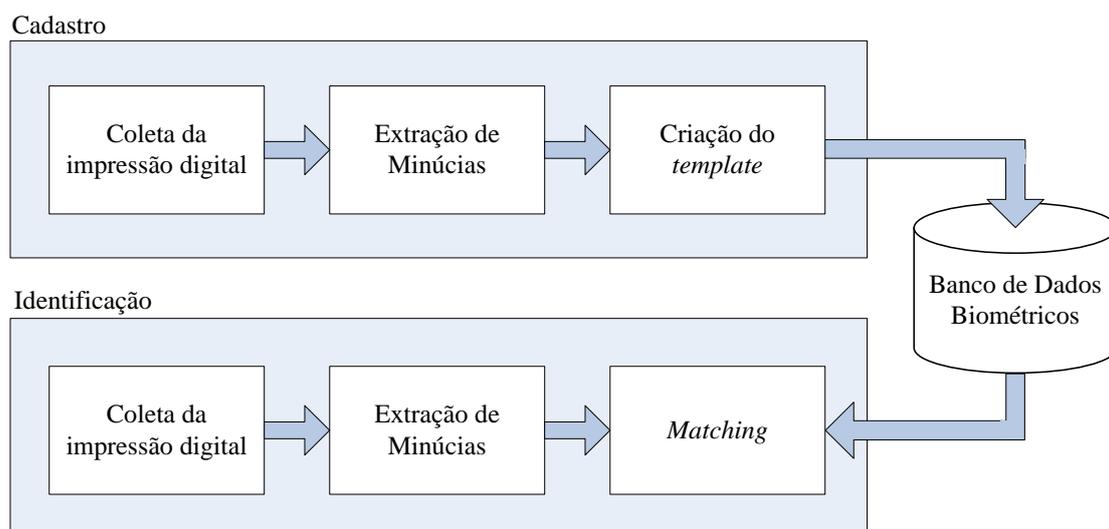


Figura 2.3 – Processo básico de um sistema de identificação de impressões digitais.

2.2.1. Cadastro

O cadastro é o processo que irá construir a base de dados de informações biométricas que será utilizado para prover o serviço de identificação. A grande maioria das técnicas de identificação biométrica de impressões digitais tem sua eficácia drasticamente degradada quando o *template* possui qualidade baixa. Por isso é muito importante que a qualidade da informação biométrica coletada no momento do cadastro

seja controlada. Principalmente quando se pretendem identificar populações muito volumosas, como a do Brasil.

2.2.1.1. Coleta da impressão digital

As atividades realizadas durante o cadastro devem, portanto, ter em vista que o objetivo é formar um banco de dados biométricos de qualidade. A coleta das impressões digitais, por exemplo, deve ser acompanhada por um técnico treinado que possa validar cada amostra coletada quanto a sua qualidade. Esta atividade pode ser apoiada por algum algoritmo que tente verificar a qualidade da impressão digital coletada. Diversos métodos já foram propostos para avaliar a qualidade de uma impressão digital coletada. Entre eles destaca-se o trabalho de *Tai Pang Che, Xudong Jiang e Wei Yun Yau* [19], que propõe uma maneira de avaliar a distinção entre os vales e as cristas (topos) associada à avaliação da fluidez da orientação das linhas (geralmente a orientação das linhas não é interrompida, a menos da existência de pontos característicos como *cores* e *deltas*). O trabalho desses autores defende, com base nos seus resultados, que esta técnica é utilizável por um AFIS.

Outra maneira de melhorar a qualidade das amostras de impressões digitais durante o processo de cadastro é utilizar mais de uma amostra para criação do *template* [20]. As características comuns à maioria das amostras obtidas são armazenadas no *template*, mas o que não for encontrado em um número significativo de amostras da mesma impressão digital é descartado, ou seja, o *template* apenas conterá os dados biométricos que se confirmam com um bom nível de confiança na amostragem realizada e tenderá a não armazenar os dados espúrios. Tais dados surgem de ruídos diversos provenientes de impurezas existentes nos dedos do indivíduo sendo cadastrado, dos sensores de amostragem (*fingerprint scanners*), dos algoritmos de extração das características (minúcias, pontos característicos etc.), entre outros.

Outro fator que influi diretamente na qualidade da impressão digital coletada é o sensor (*scanner*) utilizado. Atualmente existem diversos tipos de *scanners* de impressões digitais no mercado e várias tecnologias disponíveis. Não é do escopo deste trabalho realizar comparação ou avaliação de sensores de impressão digital, mas é interessante mencioná-los como elemento que afeta a qualidade da informação biométrica coletada.

Existem duas formas principais de coleta de uma impressão digital: a rolada e a pousada. A impressão digital pousada é capturada descansando-se o dedo sobre a superfície do sensor sem movimentá-lo. Dessa forma a imagem capturada geralmente fica com a dimensão vertical maior do que a dimensão horizontal. O sensor para este tipo de captura é mais simples e normalmente mais barato, contudo a quantidade de informação biométrica é reduzida se comparada a impressão digital rolada. A impressão digital rolada é obtida pelo rolamento do dedo sobre a superfície de coleta, tendo como eixo de rotação a falange. A imagem obtida fica com a dimensão horizontal maior e, portanto, contém mais informação biométrica. O sensor capaz de capturar impressões digitais roladas é mais caro, pois deve ser capaz de capturar a imagem da superfície do dedo em movimento sobre a área de coleta. Geralmente, o que se faz é capturar diversas imagens e sobrepô-las de forma a formar a impressão digital rolada por completo. Por capturar mais informação biométrica, a quantidade de memória necessária para armazenar uma amostra rolada e suas características é maior se comparada a uma impressão pousada para um mesmo método de extração de características.



Figura 2.4 – Impressões digitais: a) rolada b) pousada. Imagens extraídas do mesmo dedo.

Além de sensores que capturam impressões digitais roladas e pousadas, diferentes tecnologias podem ser empregadas na construção dos *scanners* que geram imagens com características um tanto diferentes (Figura 2.5). Dessa forma, a escolha de sensores que propiciem boas imagens é de grande importância para a criação de um banco de dados de informações biométricas de qualidade. Vale ressaltar ainda que, devido à diferença considerável entre as imagens coletadas por sensores diferentes, os diversos algoritmos de processamento de impressões digitais devem ser parametrizados

de forma consistente para que os resultados obtidos com sensores diferentes sejam compatíveis.



Figura 2.5 – Impressões digitais capturadas por diferentes de sensores. Da esquerda para a direita e de cima para baixo: sensor ótico “V300” da marca CrossMatch, sensor ótico “U.are.U 4000” da marca Digital Persona, sensor de varredura térmica da marca "FingerChip FCD4B14CB" da Atmel e impressão digital gerada artificialmente pelo software SFinGe v3.0 [21].

Este trabalho utiliza impressões digitais pousadas obtidas por meio de sensores óticos. Três impressões digitais de cada dedo são colhidas no momento do cadastro para aumentar a qualidade do *template* criado. A avaliação da qualidade da impressão digital coletada não foi implementada, mas sugerida para o momento da construção do AFIS em sua versão operacional.

2.2.1.2. Extração das minúcias

Historicamente, as minúcias (terminações e bifurcações) são as características mais utilizadas para realizar a comparação entre duas impressões digitais. O trabalho de um especialista não se resume a comparar minúcias, mas concentra-se em grande parte na atividade de encontrar as minúcias significativas e comparar dois conjuntos de minúcias para atestar se pertencem ou não ao mesmo dedo.

A extração automática de minúcias de uma imagem coletada por um *scanner* é classicamente formada por quatro etapas: a melhoria da imagem (*enhancement*), a binarização, o afinamento e a extração propriamente dita.

A melhoria da imagem tem por finalidade fortalecer as características da imagem necessárias os passos seguintes do processamento da imagem da impressão digital. Suavizar regiões da imagem que apresentem altas frequências (variações abruptas de cor), utilizar de forma equilibrada o espectro de valores possíveis para os pontos da imagem (normalização dos níveis de cinza) e realçar as linhas da impressão digital através de filtros passa-baixas direcionais são algumas maneiras de realizar esta tarefa [1].

Binarizar a imagem significa representá-la em apenas duas tonalidades. O processo de binarização consiste em estabelecer um limiar a partir do qual os pontos da imagem são classificados como frente ou fundo, preto ou branco. Este procedimento facilita sobremaneira as etapas posteriores da extração de informações biométricas das impressões digitais.

O processo de afinamento visa a estreitar as linhas binarizadas no passo anterior até que fiquem com a largura de 1 pixel. A imagem resultante do afinamento é chamada de esqueleto da impressão digital e representa de forma mais clara do que a imagem binarizada as estruturas das linhas que forma as impressões digitais.

Por fim, depois de afinadas as linhas da impressão digital, a localização das minúcias – extração propriamente dita – é tarefa um tanto simples. Consiste em percorrer as linhas afinadas avaliando, ponto a ponto, se há alguma interrupção. Se houver a finalização de uma linha, uma minúcia do tipo terminação é registrada e caso exista a divisão de uma linha, é anotada uma minúcia do tipo bifurcação;

Neste trabalho utilizou-se a seqüência clássica de operações para a extração de minúcias. Contudo, para cada etapa de processamento foram pesquisadas as técnicas mais recentes e mais eficientes encontradas na literatura acadêmica.

MELHORIA DA IMAGEM (ENHANCEMENT)

Atualmente, os sensores de captura de impressões digitais são capazes de obter imagens de boa qualidade, mas, ainda assim, é necessário que se realize um pré-processamento da imagem adquirida antes de realizar a binarização.

A preparação da imagem é essencial para eliminar, ao máximo possível, o ruído proveniente do *scanner* usado na sua captura. Este também é o momento apropriado para ajustar a imagem capturada a parâmetros como brilho e contraste esperados pelas etapas seguintes do processo de extração de minúcias.

Neste trabalho foram utilizadas três técnicas para realizar a melhoria da imagem: a extração dos poros contidos na imagem [6]; a suavização da imagem utilizando um filtro passa-baixas onidirecional de média móvel [7] e a filtragem da imagem por um filtro direcional do tipo passa-baixas muito utilizado para aprimorar imagens de impressões digitais, o filtro de Gabor [1].

Os detalhes da implementação do processo de extração de poros da imagem serão discutidos no Capítulo 4, mas, em linhas gerais, este algoritmo tenta eliminar os pontos claros que existem no meio das linhas escuras da imagem da impressão digital (Figura 2.9a). Estes pontos aparecem devido à presença de poros na superfície da pele os quais formam mínimos relativos às cristas das linhas da impressão digital.

O filtro de média móvel tem o objetivo de suavizar a imagem como um todo para que as pequenas discontinuidades sejam amenizadas e posteriormente eliminadas pelas outras etapas de processamento. O efeito passa-baixas também é muito interessante para as impressões digitais, pois o padrão do sinal transversal às linhas da impressão digital se aproxima mais de uma curva senoidal, que é o modelo utilizado pelas etapas posteriores de processamento, como a extração do mapa direcional, o cálculo do mapa de frequências e a filtragem de Gabor.



Figura 2.6 – Filtro de média móvel aplicado a uma impressão digital. a) imagem original e b) resultado da filtragem.

O filtro de Gabor é um filtro passa-baixas direcional. A impressão digital possui, localmente, frequência e direção constantes das linhas que a formam. Assim sendo, é possível, dividindo a imagem em setores, estimar a frequência e a direção das linhas em cada setor. Além da imagem original da impressão digital, o filtro de Gabor utiliza o mapa de frequência e o mapa direcional extraídos da imagem e, para cada setor, é realizada a filtragem das linhas da imagem com o objetivo de suavizá-las eliminando variações abruptas de frequência, que são em geral espúrias em impressões digitais. A expressão utilizada para realizar a filtragem de Gabor é a da equação (2.1).

$$g_{\lambda,\theta,\phi,\sigma,\gamma}(x, y) = \exp\left(-\frac{x'^2 + y'^2\gamma^2}{2\sigma^2}\right) \cos\left(2\pi\frac{x'}{\lambda} + \phi\right) \quad (2.1)$$

Onde:

$$\begin{aligned} x' &= x \cos(\theta) + y \sin(\theta) \\ y' &= -x \sin(\theta) + y \cos(\theta) \end{aligned}$$

Contudo, antes de se realizar a filtragem de Gabor, é necessário calcular o mapa direcional e o mapa de frequência relativos à imagem da impressão digital a ser filtrada. A técnica utilizada neste trabalho para calcular a direção e a frequência das linhas é a proposta por Shivang Patel e Jaap de Haan [7] e a implementação foi retirada do software livre FVS (*Fingerprint Verification System*).



Figura 2.7 - Impressão digital original e seu campo direcional.

Foi utilizado, ainda no pré-processamento, um modo de selecionar as partes úteis da imagem. Duas técnicas foram utilizadas para determinar se certa região da impressão digital é válida. A primeira baseia-se no desvio padrão dos valores de cinza encontrados em setores da imagem. Se o desvio padrão é maior que um dado limiar, o setor é considerado válido, caso contrário é considerado inválido. A segunda consiste em verificar setorialmente se a frequência espacial das linhas está dentro de uma faixa de frequência fixa. Essas duas técnicas foram utilizadas em conjunto (Figura 2.8) para gerar uma máscara que define a área útil a ser considerada pelo processamento realizado nas próximas etapas.

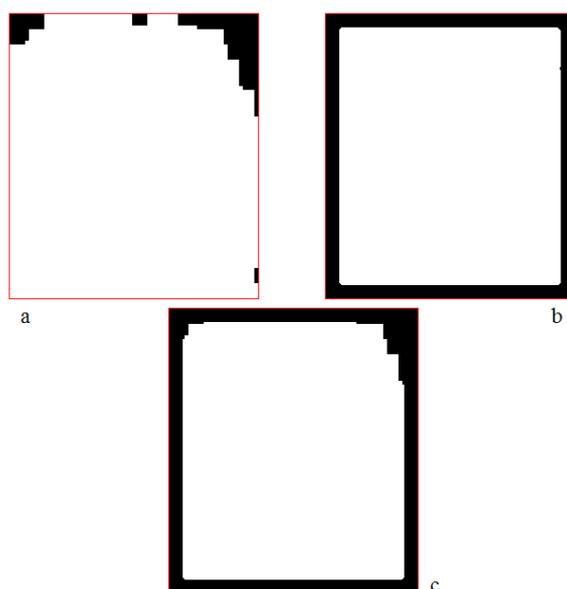


Figura 2.8 – Máscaras de definição da área útil. a) desvio padrão b) frequência c) união das duas técnicas.



Figura 2.9 – Pré-processamento. a) impressão digital original b) resultado da extração de poros c) resultado da suavização d) máscara que define a área útil e) resultado da filtragem pelo filtro de Gabor.

BINARIZAÇÃO

Esta etapa consiste em reamostrar a imagem resultante do pré-processamento com o objetivo de utilizar apenas dois tons para representá-la, geralmente preto e branco. Na seqüência de operações, esta fase é importante pois, com uma imagem em apenas dois tons, o afinamento pode ser realizado de maneira extremamente performática sob o ponto de vista de custo computacional. A Figura 2.10 ilustra o resultado desta operação: a diferença entre as figuras “a” e “b” é que na segunda existem apenas duas cores, preto e branco, e na primeira existem 256 níveis de cinza.

Neste trabalho a binarização foi realizada por meio de um limiar fixo utilizado para toda a imagem. Para o nível de cinza maior que o limiar usou-se branco, para o menor, preto.

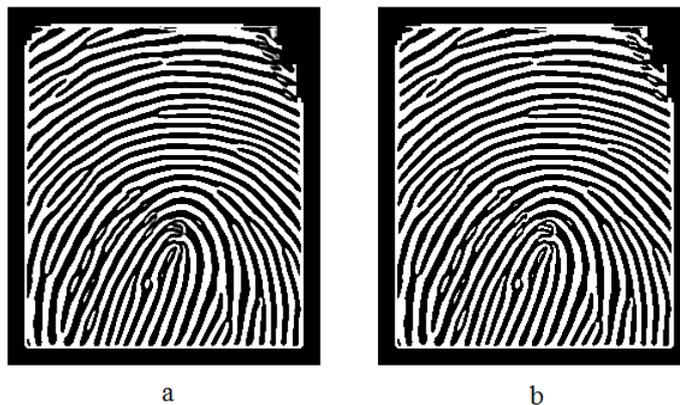


Figura 2.10 – Binarização. a) imagem resultante do pré-processamento b) imagem binarizada.

AFINAMENTO

Após a binarização, as linhas da impressão digital resultante são afinadas até possuírem largura de um ponto (um *pixel*). Existem diversos trabalhos que tratam deste algoritmo em particular, pois também há aplicação deste tipo de processamento em diversas outras áreas do processamento de imagens.

Neste trabalho foi utilizada a técnica proposta por *G.S. Ng, R.W. Zhou e C. Quek* [8], da qual não foi encontrada outra referência de utilização em processamento de impressões digitais. Esta técnica baseia-se em marcar os pontos que serão excluídos da imagem e removê-los levando em consideração não apenas a marcação mas também o resultado da iteração anterior. O resultado da aplicação deste algoritmo pode ser visualizado na Figura 2.11. Mais detalhes sobre a implementação do algoritmo de afinamento serão observados na seção 4.3.



Figura 2.11 – Impressão digital afinada.

LOCALIZAÇÃO DAS MINÚCIAS

O passo seguinte ao afinamento é a localização de minúcias. Esta etapa consiste em percorrer as linhas afinadas resultantes do processamento realizado até esse ponto para encontrar e caracterizar as discontinuidades características das minúcias de impressões digitais.

A inspeção da imagem é realizada ponto a ponto. Para todo ponto pertencente a uma linha verifica-se o número de pontos vizinhos que também pertençam à linha. Se não houver nenhum vizinho, trata-se de um ponto isolado que para este trabalho foi ignorado. Se houver apenas um vizinho, estamos diante de uma terminação de linha, ou seja, uma minúcia de terminação. Se houver dois vizinhos, estamos no meio de uma linha. Se houver três ou mais vizinhos, consideramos neste trabalho como sendo uma minúcia do tipo bifurcação. A seção 4.4 apresentará mais detalhes sobre este algoritmo e a Figura 2.12 mostra o resultado da extração de minúcias na impressão digital afinada.

Neste trabalho foi utilizada ainda uma técnica de remoção de minúcias espúrias que, freqüentemente, são encontradas nas amostras de impressão digital devido à presença de ruído nas outras etapas do processamento da imagem. A técnica utilizada aqui, além de remover as minúcias que foram encontradas na região definida como inválida pela máscara (Figura 2.9d), utiliza uma adaptação sobre o algoritmo proposto por Marius Tico e Pauli Kuosmanen [9]. Mais detalhes sobre a implementação deste algoritmo encontram-se na seção 4.4.

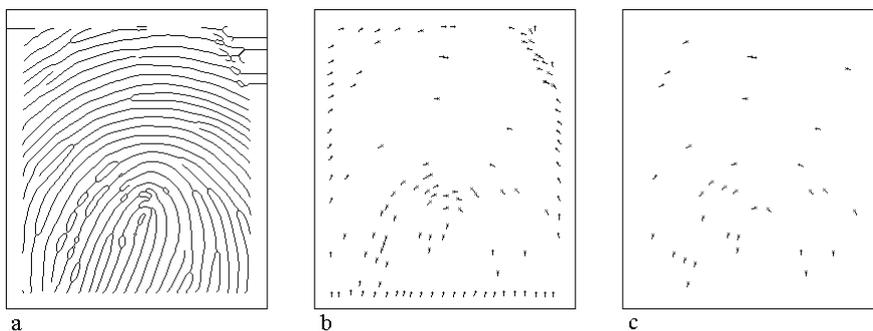


Figura 2.12 – Extração de minúcias. a) imagem afinada b) minúcias extraídas por inspeção das linhas c) minúcias que passaram pelo filtro de minúcias espúrias

2.2.1.3. Criação do template

Depois de extraídas as minúcias, é importante definir uma forma bem organizada de armazenar os dados biométricos obtidos. O padrão ISO/IEC 19794-2, que trata do formato para troca de dados biométricos de impressões digitais, foi adotado neste trabalho com o objetivo de garantir portabilidade do banco de dados biométricos gerado após a fase de cadastro.

Este padrão define dois tipos principais de formatos, um para ser utilizado em bancos de dados e aplicações convencionais e outro em cartões (*smartcards*). Neste trabalho utilizamos apenas o formato convencional. O Capítulo 3 tratará deste padrão.

No processo de criação do *template* foram utilizadas ainda duas técnicas com o objetivo de melhorar o *template*: a utilização de mais de uma amostra para o cadastro e a classificação do *template* – esta para aumentar a possibilidade de utilizar o banco de dados biométricos gerado para identificar grandes populações e aquela para aumentar a precisão dos dados contidos no *template*.

UTILIZAÇÃO DE MÚLTIPLAS AMOSTRAS PARA CRIAÇÃO DO TEMPLATE

Uma maneira eficiente de aumentar a qualidade do *template* criado é realizar a coleta de várias impressões digitais, processá-las e inserir apenas as minúcias que apareçam com determinada frequência no *template* [20].

O processo para selecionar as minúcias que serão efetivamente utilizadas consiste em: escolher, dentre as impressões digitais coletadas para o cadastro, a que possui melhor qualidade; comparar (*matching*) cada uma das outras amostras à escolhida apontando quais minúcias foram encontradas em comum e selecionar as minúcias mais votadas para compor o *template*. A Figura 2.13 ilustra este processo.

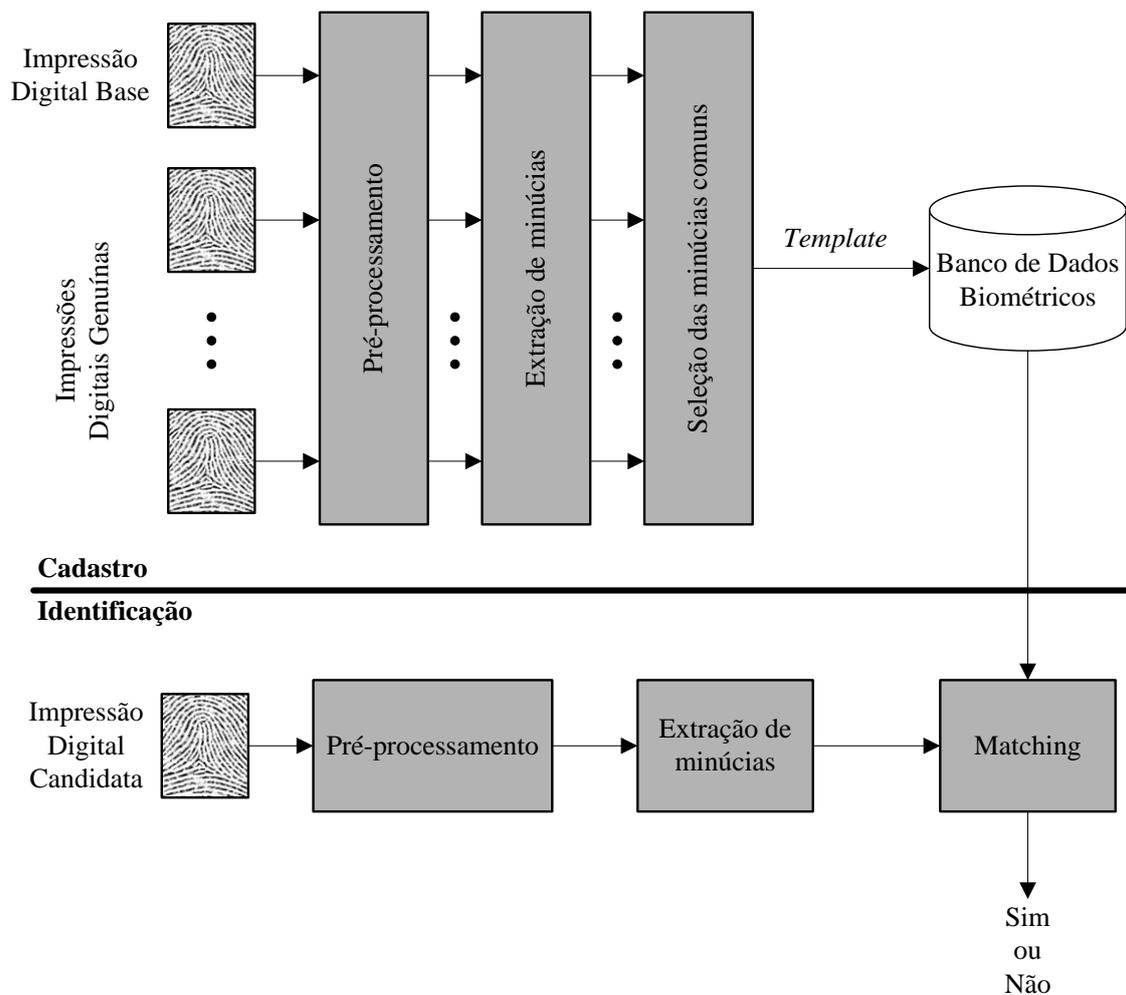


Figura 2.13 – Processo de utilização de múltiplas impressões digitais para realizar o cadastro do *template* (Fonte: [20]).

CLASSIFICAÇÃO

Outro fator a ser considerado aqui é que o banco de dados a ser criado utilizando a técnica aqui proposta deverá ser utilizado para a identificação de uma grande população. Quando o conjunto de impressões digitais cadastradas é muito grande, o processo de identificação de uma impressão digital candidata pode ser extremamente demorado.

Uma forma de diminuir a quantidade de registros pesquisados em um processo de identificação (comparação 1:n) é classificar os registros contidos no banco para que apenas aqueles pertencentes à classe da impressão digital candidata sejam consultados. Por exemplo: se houver a informação de que a impressão digital candidata pertence a

uma mulher, pode-se eliminar do processo de identificação todas as impressões digitais que pertençam a homens. Para isso, a informação sobre o sexo do indivíduo deve ser conhecida, e essa informação não faz parte dos dados biométricos de impressão digital. Quando a identificação deve ser processada possuindo-se apenas a impressão digital candidata esta classificação não traz economia alguma.

Contudo, é possível realizar a classificação de impressões digitais utilizando-se apenas as características presentes nas imagens coletadas. Existem diversas técnicas criadas com este objetivo, destacando-se entre elas as propostas em [22] [23] [24] [25] [26] [27] [28] [29] [30].

A técnica escolhida utiliza a compartimentalização dos campos direcionais obtidos a partir da imagem da impressão digital para classificá-la em: arco (*arch*), arco apoiado (*tented arch*), laço esquerdo (*left loop*), laço direito (*right loop*) e ninho (*whorl*) (Figura 2.14). Utilizando-se essas cinco classes é possível diminuir o espaço de busca de uma impressão digital em até 80%, pois apenas um quinto das impressões digitais cadastradas deverá ser efetivamente pesquisado.

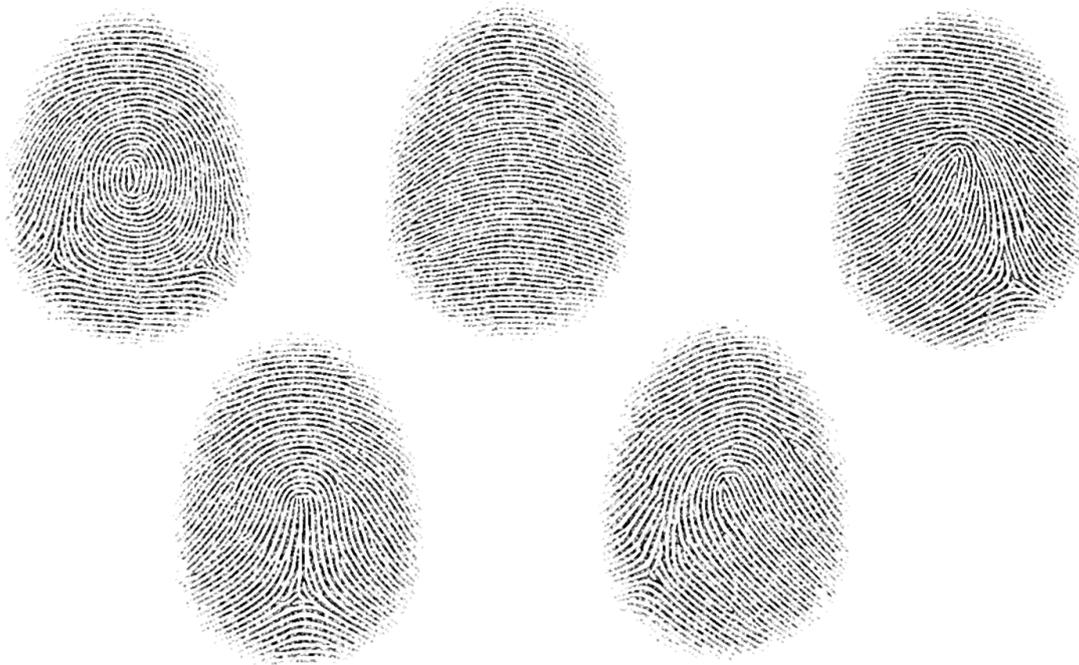


Figura 2.14 – Exemplos de impressões digitais pertencentes às classes consideradas pela técnica utilizada. Da esquerda para a direita, na primeira linha: ninho, arco e laço esquerdo; na segunda linha: arco apoiado e laço direito.

A compartimentalização dos campos direcionais é realizada utilizando-se uma máscara dinâmica pré-definida para cada uma das classes. Cada máscara dinâmica define regiões do campo direcional onde a variação da direção seja a menor possível. As classes e as respectivas máscaras consideradas neste trabalho foram as apresentadas em [31]. A Figura 2.15 ilustra as máscaras que foram construídas para classificar as impressões digitais utilizadas neste trabalho.

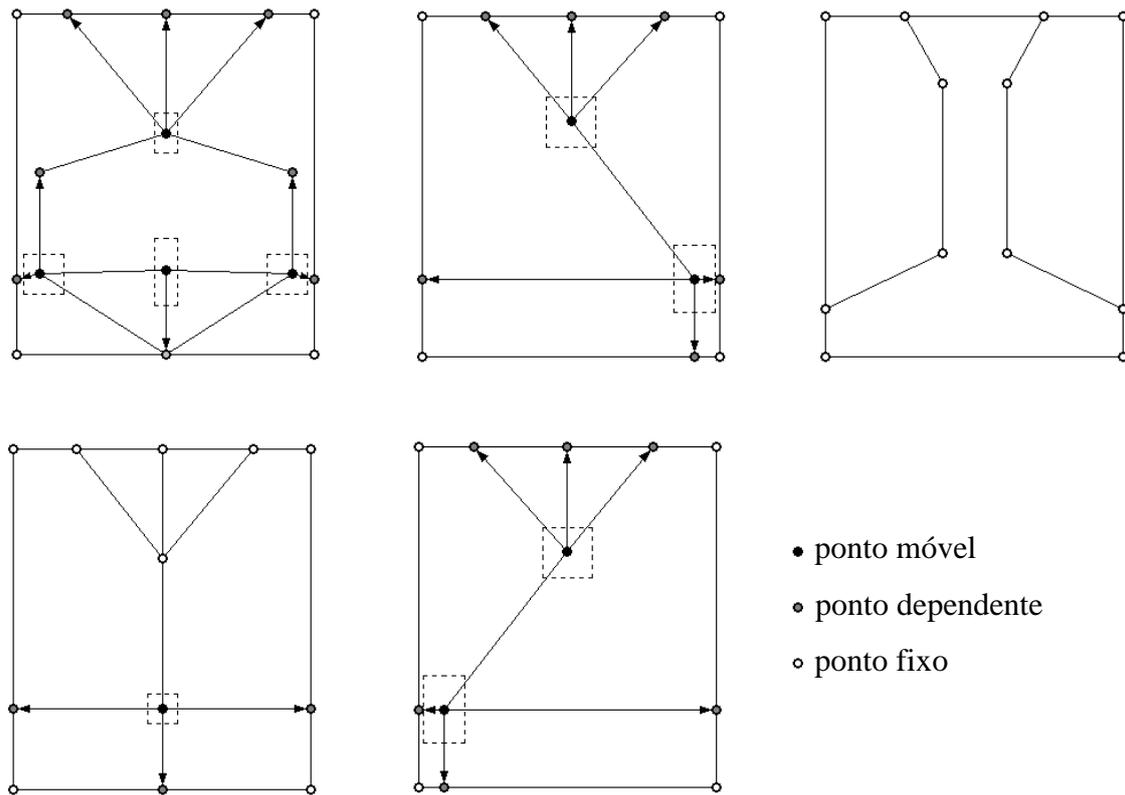


Figura 2.15 – Máscaras dinâmicas do algoritmo de classificação. Da esquerda para a direita, de cima para baixo: ninho, laço esquerdo, arco, arco apoiado e laço direito.

A máscara é ajustada dentro dos limites estabelecidos para a movimentação dos seus pontos móveis. Assim sendo, uma máscara M sofre inicialmente uma rotação Q e uma translação T . Para realizar o ajuste, o custo de aplicação da máscara é calculado pela equação (2.2).

$$C_{sm}(M_{T,Q}, Dir) = \sum_{i=1}^n [C_0 + Var(R_i)] + \mu \cdot \frac{1}{card(A)} \cdot \sum_{(P_i, P_j, \theta_{ij}) \in A} \Delta abs[\Delta dir(R_i, R_j), \theta_{ij}] \quad (2.2)$$

Onde: $Var(R_i)$ é proporcional à variância dos elementos direcionais que compõem a região R_i ; C_0 é um parâmetro que penaliza as máscaras que possuem mais regiões, pois essas máscaras possuem maior probabilidade de produzir menores custos [32]; $\Delta dir(R_i, R_j)$ é a diferença entre os valores médios dos elementos direcionais que compõem as regiões R_i e R_j ; $\Delta abs(\theta_i, \theta_j)$ resulta na diferença entre θ_i e θ_j convertido ao intervalo $[-90^\circ, 90^\circ]$; μ é o peso do termo relativo à diferença entre as orientações médias; A é um conjunto que contém as triplas constituídas por um par de regiões da máscara e a diferença esperada entre as orientações médias dessas regiões; e, por fim, $card(A)$ retorna o número de triplas contidas em A .

Para definir o custo final da aplicação da máscara, uma seqüência de operações é realizada: a máscara é rotada, depois deslocada, a seguir os pontos móveis são deslocados dentro de sua janela de movimentação – os pontos dependentes deslocam-se seguindo a movimentação dos pontos móveis que referenciam. Para cada configuração da máscara o custo é calculado, e o menor valor encontrado é considerado o custo final de aplicação da máscara.

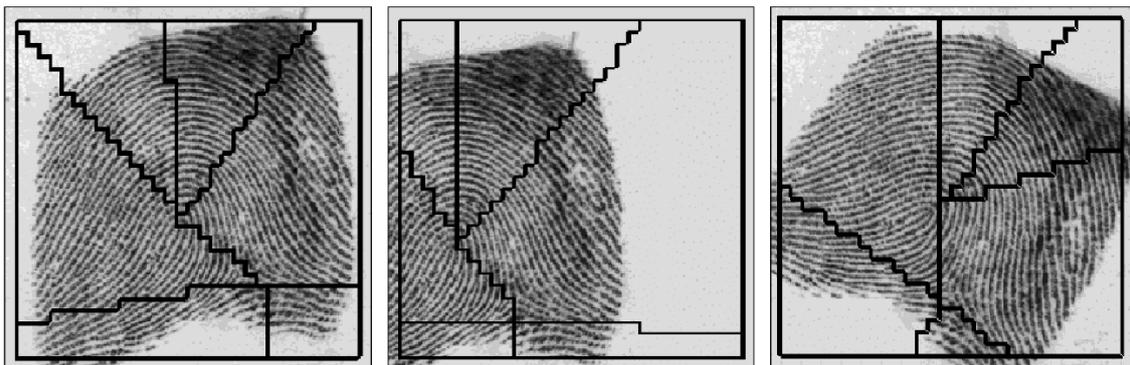


Figura 2.16 – Exemplo de adaptação de máscara dinâmica a uma impressão digital da classe laço esquerdo (Fonte: [31])

2.2.2. Identificação

O processo de identificação é realizado quando o AFIS for integrado a alguma aplicação ou a algum sistema para realizar o papel de autenticador. Ou seja, depois de realizado o cadastro, o banco de dados biométricos de impressões pode ser utilizado para realizar a autenticação de indivíduos por meio de suas impressões digitais. A Figura 2.3 mostra que a diferença entre o processo de identificação e o de cadastro é que ao final da identificação, em vez de criar um *template* para ser armazenado, o AFIS realiza a comparação entre o conjunto de minúcias candidato e o *template* armazenado no banco de dados.

Nos casos onde a identidade do indivíduo é conhecida, o AFIS deverá apenas confirmar que a impressão candidata é realmente pertencente a esse indivíduo. Este tipo de comparação de impressões digitais é chamado de um para um (1:1), pois compara-se a impressão digital candidata apenas com o *template* referente à identidade daquele indivíduo. Este processo é também chamado correntemente, na literatura, de verificação.

Por outro lado, se a identidade do indivíduo do qual se coletou a impressão candidata é desconhecida, o AFIS deverá pesquisar o banco de dados e verificar, dentre as impressões digitais cadastradas, se alguma corresponde à impressão procurada. Este processo é também conhecido por identificação ou comparação um para n (1:n). Geralmente a comparação 1:n é implementada através de n comparações 1:1.

MATCHING

Neste trabalho foi implementado um algoritmo de *matching*, que utiliza a transformada de Hough [33] para realizar a comparação entre dois conjuntos de minúcias. As transformações de Hough utilizadas são a rotação e a translação. A escala também é uma transformação do espaço de Hough, mas, como as imagens de impressões digitais coletadas possuem a mesma resolução, não foi necessário considerar esta transformação. Os detalhes da transformada de Hough estão no Anexo A.

Para facilitar a compreensão, as seguintes nomenclaturas foram utilizadas: o conjunto de minúcias do *template* é representado por *I* e cada minúcia deste conjunto é

representada por m_i ; o conjunto de minúcias da impressão digital candidata é representado por C e cada minúcia deste conjunto é representada por m_c ; o conjunto dos ângulos para os quais C será rotado é θ e cada valor pertencente a este conjunto é θ_r ; os conjuntos dos deslocamentos horizontais e verticais que serão considerados para a translação de C são, respectivamente, Dx e Dy , e os valores assumidos para as translações representam-se por Dx_t e Dy_t .

Um conjunto \mathcal{H} das transformações realizadas em C pode ser definido para conter a quantização realizada para cada transformação considerada. Ou seja, $\mathcal{H}(C, Dx, Dy, \theta)$ conterá uma entrada para cada valor quantizado de Dx_t , Dy_t e θ_r utilizado na transformação de C . A cada transformação realizada – $\mathcal{H}(C, Dx_t, Dy_t, \theta_r)$ – é associada uma pontuação relativa à quantidade de minúcias emparelhadas entre P e $\mathcal{H}(C, Dx_t, Dy_t, \theta_r)$.

Respeitados limiares de rotação – θ_0 – e translação – D_{t0} – para m_c , uma minúcia $m_i \in I$ é considerada emparelhada a $m_c \in C$ quando ambas possuírem mesma posição espacial e mesma direção. A Figura 2.17 ilustra o emparelhamento de uma minúcia candidata a uma minúcia do *template*, segundo essa definição.

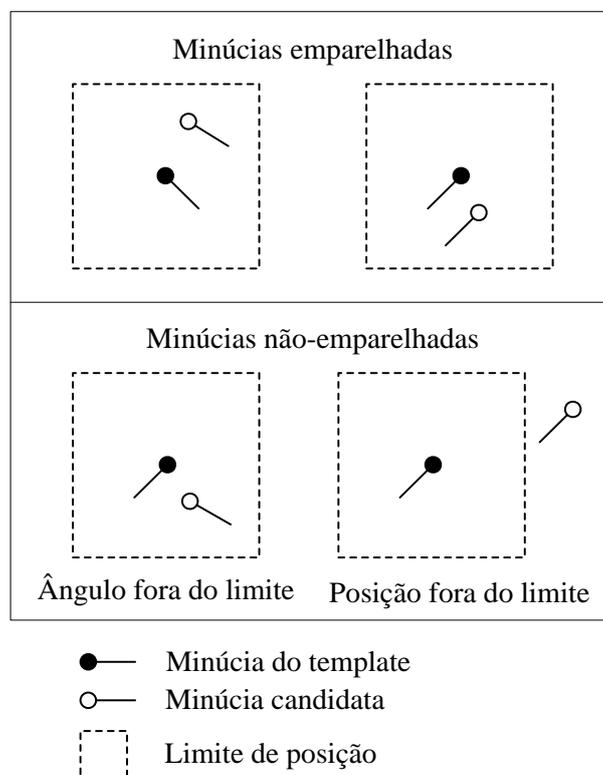


Figura 2.17 – Emparelhamento de minúcias (Fonte: [33] com alterações).

Seguindo a notação sugerida, o pseudocódigo para o algoritmo de alinhamento dos dois conjuntos de minúcias, *template* e candidata, apresenta-se a seguir:

Algoritmo 1 – Processo de *matching* utilizado.

<p> <i>Para cada</i> $m_i(x_i, y_i, \alpha_i) \in I$ <i>Para cada</i> $m_c(x_c, y_c, \beta_c) \in C$ <i>Para cada</i> $\theta_r \in \theta$ <i>Se</i> $\alpha_i - (\beta_c - \theta_r) \leq \theta_0$ $\begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} := \begin{bmatrix} x_i \\ y_i \end{bmatrix} - \begin{bmatrix} \cos \theta_r & -\sin \theta_r \\ \sin \theta_r & \cos \theta_r \end{bmatrix} \begin{bmatrix} x_c \\ y_c \end{bmatrix}$ <i>Se</i> $(\Delta x \in D_x)$ e $(\Delta y \in D_y)$ Adicionar 1 ao valor de $\mathcal{H}(C, Dx_t, Dy_t, \theta_r)$ <i>Fim para cada</i> θ_r <i>Fim para cada</i> m_c <i>Fim para cada</i> m_i <i>Resultado</i> $:= \arg \max_{i,c,r} \mathcal{H}(C, Dx, Dy, \theta)$ </p>

O resultado do algoritmo acima é o conjunto de transformações realizadas em C que produz o maior número de minúcias emparelhadas. Resta ainda finalizar o processo de *matching* e estabelecer se I e C podem ser considerados como pertencentes à mesma impressão digital.

Um limiar mínimo de emparelhamento das minúcias deve ser atingido para que o algoritmo de *matching* considere a comparação realizada como bem sucedida. O limiar utilizado neste trabalho foi de 50 % do número de minúcias do *template* para o *matching* 1:1.

Porém, quando se trata da comparação 1:n, esse limiar define apenas o mínimo necessário para que se considere que a impressão candidata pertença ao banco de *templates*, ou seja, se algum dos *templates* armazenados for emparelhado com a candidata em mais de 50%, considera-se que existe pelo menos uma impressão digital no banco que corresponde à candidata. Desta forma, os melhores emparelhamentos são considerados como corretos e retornados como resultado da busca em um máximo de 10 *templates* por identificação.

3. PADRÕES INTERNACIONAIS CONSIDERADOS

Para criação de um processo de cadastro que produza um banco de dados de boa qualidade, é necessário considerar os padrões que se aplicam tanto ao processo quanto ao armazenamento dos dados biométricos. Este capítulo contém uma breve descrição dos padrões levados em conta no presente trabalho.

Dois padrões internacionais foram considerados importantes para que o cadastro realizado apresente boa portabilidade. Para o armazenamento dos dados foi escolhido o padrão ISO/IEC 19794-2, que define um formato para comunicação de dados biométricos de impressões digitais baseados em minúcias. Quanto ao processo de cadastro, foi selecionado um padrão que define uma interface para o desenvolvimento de aplicações que utilizam biometria e cobre de forma muito concisa e organizada as funcionalidades envolvidas em tais aplicações – a BioAPI.

3.1. ISO/IEC 19794-2

Diversos formatos podem ser utilizados para a comunicação de dados coletados a partir de impressões digitais. Contudo, pode ocorrer um gasto excessivo dos meios de transmissão e armazenamento envolvidos em um sistema de identificação biométrica caso a informação coletada não seja corretamente dimensionada. E mais, a troca de informações entre sistemas de identificação biométrica é uma necessidade comum sempre que há interação que troque informação biométrica entre os sistemas.

A norma ISO/IEC 19794-2 define um formato bastante interessante para a troca de informações biométricas de impressões digitais baseadas em minúcias. Esse formato utiliza uma terminologia básica onde cada registro pode conter múltiplas visões de dedos (*finger views*) que, por sua vez, possuem várias minúcias e informações estendidas. Dessa forma, cada visão de dedo traz as informações obtidas a partir de uma imagem de impressão digital, quais sejam: minúcias, pontos característicos, informações de qualidade e outros. As visões de dedos são agrupadas para formar os registros. O formato resumido do registro de minúcias é apresentado na Tabela 2.1.

Tabela 2.1 – Resumo do formato do registro de minúcias (fonte: [11] traduzida).

		Campo	Tamanho	Valores válidos	Observações
Um por registro		Identificador de formato	4 bytes	0x464D5200 (‘F’‘M’‘R’ 0x0)	“FMR” – finger minutiae Record
		Versão deste padrão	4 bytes	n n n 0x0	“ XX”, com XX = 20 ou maior
		Comprimento total do registro em bytes	4 bytes	24 – 4294967295	De 0x0018 a 0x0000FFFFFFFF
		Certificação do equipamento de captura	4 bits		Segundo Anexo B ou futura norma ISO
		ID do tipo de dispositivo de captura	12 bits		Especificado pelo fabricante
		Tamanho da imagem em X	2 bytes		Em <i>pixels</i>
		Tamanho da imagem em Y	2 bytes		Em <i>pixels</i>
		Resolução em X (horizontal)	2 bytes		Em pixels por cm
		Resolução em Y (vertical)	2 bytes		Em pixels por cm
		Número de visões de dedos (<i>finger views</i>)	1 byte	0 a 255	
	Byte reservado	1 byte	00	0 para esta versão do padrão (reservado para uso futuro)	
Um por visão		Posição do dedo	1 byte	0 a 10	Tabela 2.2
		Número da visão	4 bits	0 a 15	
		Tipo de impressão	4 bits	0 a 3 ou 8	Tabela 2.3
		Qualidade do dedo	1 byte	0 a 100	
		Número de minúcias	1 byte		
Um por minúcia		X (tipo da minúcia nos dois bits superiores)	2 bytes		Em <i>pixels</i>
		Y (dois bits superiores reservados)	2 bytes		Em <i>pixels</i>
		θ	1 byte	0 a 255	Resolução de 1,40625 graus
		Qualidade	1 byte	0 a 100	1 a 100 (0 significa qualidade desconhecida)
Um por visão		Comprimento do bloco de dados estendidos	2 bytes		0x0000 = sem área privada
0+ por visão		Código do tipo de área de dados estendidos	2 bytes		Tabela 2.4, presente apenas se o comprimento dos dados estendidos ≠ 0
		Comprimento da área de dados estendidos	2 bytes		Presente apenas se o comprimento do bloco de dados estendidos ≠ 0
		Dados estendidos	No campo anterior		Presente apenas se o comprimento do bloco de dados estendidos ≠ 0
Cada área de dados estendidos pode conter dados do fabricante ou um ou mais dos seguintes (em qualquer ordem):					
0+ por visão	Contagem de linhas	Método de extração da contagem de linhas	1 byte	0 a 2	
		Dado de contagem de linha – idx #1	1 byte	1 ao # de minúcias	
		Dado de contagem de linha – idx #2	1 byte	1 ao # de minúcias	
		Dado de contagem de linha – núm.	1 byte		
		<i>contagem adicional de linhas...</i>			
	Dados de core e delta	Número de cores	4 bits	0 a 15	
		Tipo de informação de core	2 bits	0 a 1	
		Posição X	14 bits		
		Posição Y	2 bytes		
		Ângulo (p/ tipo de info. de core ≠ 0)	1 byte	0 a 255	
		Número de deltas	4 bits	0 a 15	
		Tipo de informação de delta	2 bits	0 a 1	
		Posição X	14 bits		
		Posição Y	2 bytes		
Ângulos (p/ tipo de info. de delta ≠ 0)	3 byte	0 a 255			
0+ por visão	Qualidade por zona	Largura da célula	1 byte	1 a 255	
		Altura da célula	1 byte	1 a 255	
		Informação do número de bits da célula	1 byte	1 a 255	
		Dados de qualidade da célula	# de bits da célula		

Tabela 2.2 – Códigos das posições dos dedos.

Posição do dedo	Código
Dedo desconhecido	0
Polegar direito	1
Indicador direito	2
Médio direito	3
Anelar direito	4
Mínimo direito	5
Polegar esquerdo	6
Indicador esquerdo	7
Médio esquerdo	8
Anelar esquerdo	9
Mínimo esquerdo	10

Tabela 2.3 – Códigos dos tipos de impressões.

Descrição	Código
<i>Live-scan</i> pousada	0
<i>Live-scan</i> rolada	1
Imagem pousada	2
Imagem rolada	3
<i>Latent impression</i>	4
<i>Latent tracing</i>	5
<i>Latent photo</i>	6
<i>Latent lift</i>	7
Varredura	8

Tabela 2.4 – Códigos de tipos de dados estendidos

Primeiro byte	Segundo byte	Tipo de dados estendidos
0x00	0x00	reservado
0x00	0x01	dados de contagem de linhas
0x00	0x02	dados de <i>core</i> e delta
0x00	0x03	dados de qualidade por zona
0x00	0x04 a 0xFF	reservado
0x01 a 0xFF	0x00	reservado
0x01 a 0xFF	0x01 a 0xFF	dados estendidos de fabricantes

A norma ISO/IEC 19794-2 não prevê um formato específico para a representação da classe a que a visão do dedo pertence, contudo existe a possibilidade de utilizar o campo de dados estendidos para este propósito. A Tabela 2.5 apresenta uma

proposta para a representação da classe a que a impressão digital pertence. Essa proposta foi concebida ao longo do desenvolvimento deste trabalho.

O formato proposto (Tabela 2.5) deve ser utilizado na seção referente aos dados estendidos da visão de dedo. Contudo, tendo em vista que a classificação da impressão digital é essencial para a utilização de biometria de impressões digitais na identificação de grandes populações e que esse tipo de aplicação se beneficia indubitavelmente da padronização proposta pela norma ISO/IEC 19794-2, é interessante que os dados relativos à classe da visão de dedo possuam um código bem definido. A proposta deste trabalho é que o código 0x0004 seja utilizado para este fim.

Tabela 2.5 – Proposta de formato para a classe da visão de dedo.

	Campo	Tamanho	Valores válidos	Observações
0+ por visão	Método de classificação	1 byte	1 a 255	0x00 – Método indefinido 0x01 – Classificação por pontos característicos 0x02 – Particionamento do campo direcional 0x03 – Classificação por rede neural 0x04 a 0xFF – reservado para uso futuro
	Número de classes	1 byte	2 a 255	Número de classes utilizadas
	Pontuação Classe 1 ou Pontuação laço esquerdo	1 byte	1 a 100	0x00 – pontuação indefinida; 0xFF – classe selecionada
	Pontuação Classe 2 ou Pontuação laço direito	1 byte	1 a 100	
	Pontuação Classe 3 ou Pontuação arco	1 byte	1 a 100	
	Pontuação Classe 4 ou Pontuação arco apoiado	1 byte	1 a 100	
	Pontuação Classe 5 ou Pontuação ninho	1 byte	1 a 100	
	Pontuação Classe 6	1 byte	1 a 100	
	
Pontuação Classe N (1 < N < 256)	1 byte	1 a 100		

Os métodos de classificação considerados – códigos 0x01, 0x02 e 0x03 – foram escolhidos com base nas técnicas mais comumente encontradas nos trabalhos recentes sobre classificação de impressões digitais. A informação do número de classes deve ser utilizada para calcular o comprimento em bytes do bloco de dados de classificação. O número de classes depende do método de classificação selecionado. Alguns métodos utilizam um número grande de classes as quais não mostram relação direta com a disposição das linhas da impressão digital; contudo, grande parte dos métodos utiliza as classes empregadas neste trabalho por se tratar de classes consolidadas na literatura, que possuem boa representatividade no espectro de impressões digitais.

Após o campo de número de classes seguem-se as informações sobre a classe propriamente dita. A maioria dos métodos de classificação permite estabelecer uma pontuação para as classes consideradas. Nesses casos cada classe recebe uma pontuação e a de maior pontuação é considerada a classe à qual a impressão digital pertence. No entanto, alguns métodos retornam uma classificação única para a impressão digital considerada. Assim, o valor 0xFF – em hexadecimal – deve ser associado à classe da impressão digital. Às demais classes deve-se associar o valor 0x00.

3.1. BioAPI

Atualmente, existem diversos padrões internacionais de terminologias, modelos e interfaces utilizados para desenvolver softwares relacionados à biometria. Contudo, há um padrão de interface para aplicações que utilizam biometria que vem-se tornando muito respeitado na comunidade desenvolvedora, a BioAPI.

Este padrão define uma interface para o desenvolvimento de aplicações que utilizam biometria e cobre de forma muito concisa e organizada as funcionalidades envolvidas em tais aplicações. Baseia-se nos três processos principais utilizados neste tipo de aplicação, quais sejam: o processo de cadastro, chamado de *Enroll*; o processo de verificação, chamado de *Verifying*; e o processo de identificação, chamado de *Identifying*.

A partir desses três processos principais a BioAPI define um *framework* que provê funcionalidades para utilizar qualquer tipo de biometria de modo transparente para a aplicação que a utiliza. Este *framework* é voltado para desenvolvimento de aplicações cliente-servidor, mas também pode ser utilizado para o desenvolvimento de aplicações *stand-alone*.

A BioAPI fornece uma série de interfaces para utilização deste framework [12]. Mas, para o escopo deste trabalho, importa a interface proposta para as funções de biometria.

As principais funções da interface de biometria são:

- BioAPI_Capture;

- BioAPI_CreateTemplate;
- BioAPI_Enroll;
- BioAPI_Verify;
- BioAPI_Identify.

A função BioAPI_Capture oferece a interface com os dispositivos de captura de dados biométricos como scanners de impressões digitais, scanners de íris, etc. A função BioAPI_CreateTemplate processa os dados obtidos dos sensores de biometria e os transforma em um *template*. A função BioAPI_Enroll realiza o processo de cadastro de um indivíduo por completo, incluindo a captura da biometria e a criação do *template*. A função BioAPI_Verify realiza o *matching* 1:1. A função BioAPI_Identify realiza o *matching* 1:N. A Figura 2.18 exibe a estrutura da aplicação de biometria básica considerada pela BioAPI 1.1.

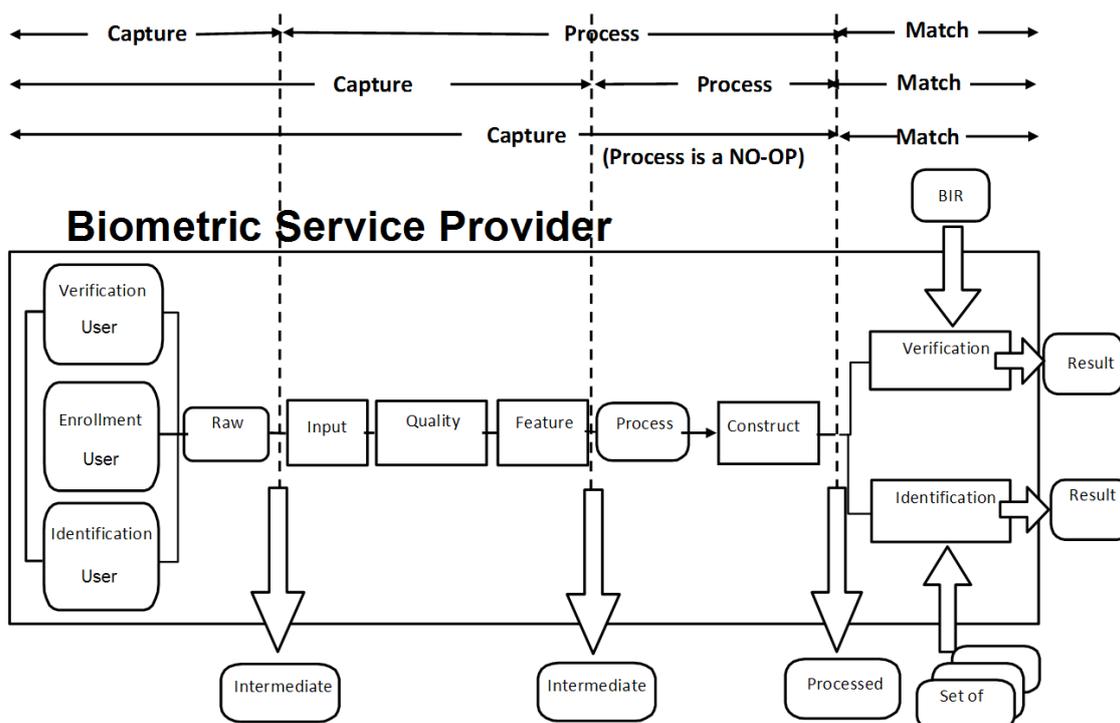


Figura 2.18 – Estrutura de uma aplicação de biometria (fonte: [12])

A BioAPI foi desenvolvida inicialmente por um consórcio de empresas e organizações interessadas na área de identificação biométrica – o BioAPI Consortium. Atualmente existem duas versões diferentes da BioAPI, a 1.1 e a 2.0. A primeira é um

padrão ANSI (*American National Standard Institute*) e a segunda se tornou um padrão ISO/IEC em 2006 (ISO/IEC 19784-1:2006).

A BioAPI 1.1 apresenta o mesmo conteúdo da especificação original desenvolvida pelo *BioAPI Consortium*. A versão 2.0 é uma versão completamente nova, desenvolvida pelo Comitê de Padrões Internacionais para Biometria, que é interno à ISO (ISO/IEC JTC1 SC37).

Este trabalho foi planejado para atender à BioAPI 1.1. Apesar da versão 2.0 ser mais moderna e apresentar diversas melhorias, este trabalho não tem o escopo de migrar a interface desenvolvida para a versão mais recente, mas sim de indicar qual padrão deverá ser seguido no caso de se utilizar o conhecimento aqui agrupado para o desenvolvimento de uma aplicação de fato. Contudo, o BioAPI Consortium sugere veementemente que esta migração seja feita para acompanhar o trabalho de padronização realizado pelo SC37, que vem criando diversos padrões relacionados à utilização de biometria baseados na BioAPI 2.0 [34].

4. IMPLEMENTAÇÕES E TESTES

Algumas melhorias foram propostas para os algoritmos utilizados no cadastro de impressões digitais. Este capítulo exporá essas melhorias e as implementações realizadas para cada processamento efetuado no cadastro da impressão digital.

O processamento da impressão digital para o cadastro segue a seqüência básica mostrada na Figura 2.3. Contudo, em mais detalhes, o processamento da imagem da impressão digital após sua captura é composto de diversos algoritmos que realizam operações bem definidas e seqüenciadas, como foi mostrado nas seções 2.2.1.2 e 2.2.1.3. Essas operações têm o objetivo de criar um registro em um banco de dados biométricos que contenha a informação necessária para prover o serviço de identificação biométrica por impressões digitais.

Assim, segue-se o detalhamento de algumas das seguintes operações: extração de poros, suavização por filtro de média móvel, cálculo do campo direcional, cálculo do mapa de freqüência, definição da área útil (máscara), filtragem de Gabor, binarização, afinamento, extração das minúcias e filtragem de minúcias falsas. A Figura 4.1 e a Figura 4.2 ilustram a seqüência destas operações:

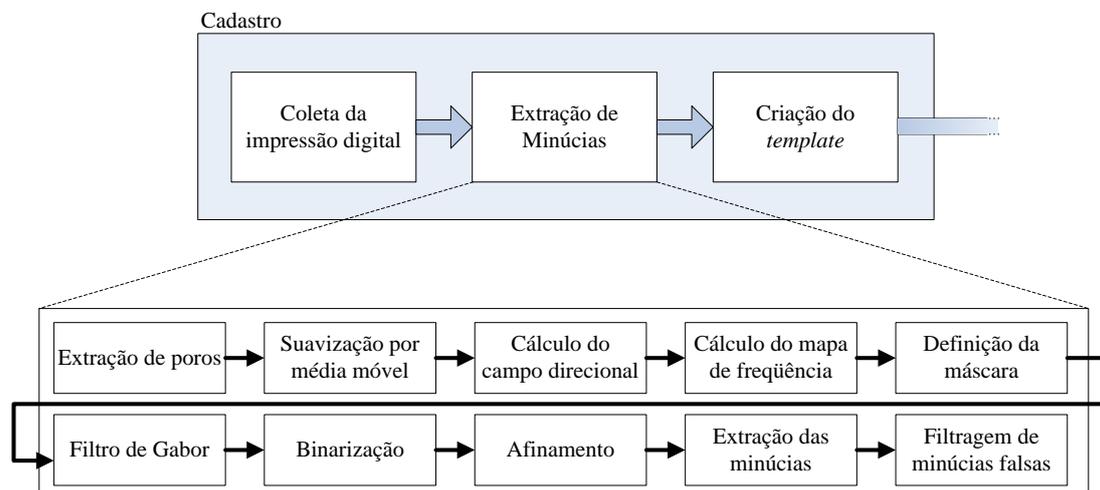


Figura 4.1 – Detalhamento das operações realizadas para o processamento da imagem da impressão digital coletada.

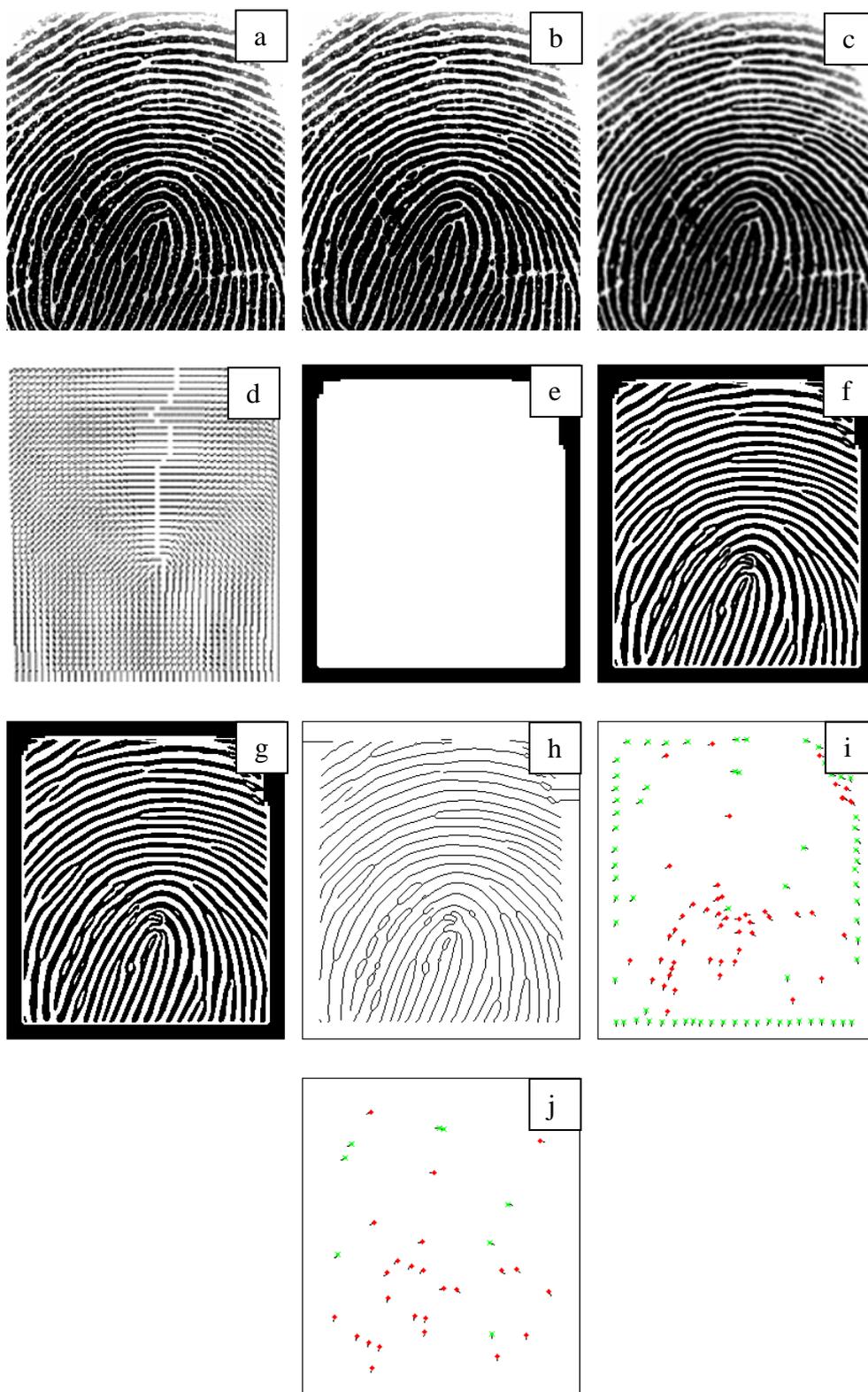


Figura 4.2 – Operações realizadas para o cadastro de uma impressão digital. As imagens ilustram os seguintes processos: a) imagem original capturada, b) extração de poros, c) suavização por filtro de média móvel, d) cálculo do campo direcional, e) definição da área útil (máscara), f) filtragem de Gabor, g) binarização, h) afinamento, i) extração das minúcias e j) filtragem de minúcias falsas.

Com o objetivo de validar as propostas descritas neste Capítulo e de gerar parâmetros de avaliação do banco de dados de informações biométricas de impressões digitais, uma biblioteca de software foi criada e seu desempenho foi testado quanto à criação de um banco de dados de registros de minúcias (ver seção 3.1) de boa qualidade.

A qualidade de um banco de dados biométricos de impressões digitais pode ser avaliada pela proporção de minúcias verdadeiras com relação à quantidade total de minúcias armazenadas por impressão digital. Pode-se avaliar a qualidade também pela quantidade de minúcias verdadeiras encontradas comparada à quantidade de minúcias existentes na imagem. Podem ser definidos ainda valores médios e desvios padrão para essas quantidades para estabelecer medidas de robustez da técnica adotada.

Diante disso, este trabalho norteou os testes realizados pela métrica de minúcias falsas em proporção ao total de minúcias detectadas. Esta medida fornece uma boa avaliação da qualidade da técnica de cadastro de informações biométricas de impressões digitais, pois reflete bem a qualidade dos *templates* armazenados no banco de dados criado.

Cabe frisar, contudo, que a métrica utilizada é dispendiosa, pois, para o banco de impressões digitais escolhido para a realização dos testes (DB1 da FVC2004), exige que seja verificada visualmente a veracidade de cada minúcia encontrada. Esta tarefa é penosa e demanda tempo, mas o foco deste trabalho não está no processo de identificação biométrica como um todo, mas apenas na fase de cadastro. Assim, utilizar as técnicas mais comuns de avaliação como valores de FAR – *False Acceptance Rate* –, FRR – *False Rejection Rate* – ou curvas ROC – FAR x FRR – acrescentaria imprecisões nas medidas uma vez que essas são baseadas nos resultados das comparações (*matchings*) realizadas na fase de identificação, que não foi detalhada neste trabalho por não ser este seu escopo (para mais detalhes sobre as métricas de FAR, FRR e curvas ROC, ver [10], [35], [36], [37], [18] e [15]).

Outra característica importante dos testes realizados é o banco de imagens de impressões digitais utilizado. Como exposto na seção 2.2.1.1, as características da imagem coletada podem variar sobremaneira de um sensor para outro. Dessa forma, decidiu-se utilizar um banco de impressões digitais cujas imagens foram coletadas com o mesmo sensor. Este conjunto de impressões digitais é bem conhecido e muito

utilizado acadêmica e comercialmente para validação de técnicas de reconhecimento de impressões digitais. Trata-se do banco 1 – DB1 – utilizado na FVC2004 – *Fingerprint Verification Competition* 2004. A Figura 4.3 mostra seis exemplos de imagens de impressões digitais contidas nesse banco.



Figura 4.3 – Exemplos de imagens contidas no banco de impressões digitais DB1 da FVC2004. À esquerda, duas imagens de boa qualidade; ao centro, duas de qualidade regular; e à direita, duas de má qualidade.

O banco DB1 da FVC2004 contém imagens capturadas a partir de 100 dedos diferentes, sendo 8 amostras diferentes para cada dedo, totalizando 800 imagens. As imagens deste banco foram capturadas com um sensor ótico [5]. Este banco é composto por arquivos codificados no formato TIFF (*Tagged Image File Format*), que é um formato de arquivos de imagem sem compactação.

O padrão de nomenclatura dos arquivos contidos nos bancos da FVC2004 é bem simples. Trata-se de dois números inteiros, separados por um *underscore*, seguidos da extensão “.tif”, por exemplo: “40_5.tif”. O primeiro número indica o dedo a partir do qual a imagem foi coletada e o segundo o número da amostra referente a esse dedo, ou seja, no exemplo citado, a imagem é referente à quinta amostra coletado do quadragésimo dedo. Além dessa informação, não há nenhum outro dado sobre as imagens pertencentes ao banco, o que significa que não são conhecidas nem a posição nem a quantidade das minúcias supostamente reais nas imagens.

4.1. EXTRAÇÃO DE POROS

Como já foi dito anteriormente, a extração de poros consiste em eliminar os pontos brancos da imagem da impressão digital, uma vez que esses pontos correspondem aos poros da pele. O algoritmo utilizado aqui é baseado no trabalho de Michael Ray, Peter Meenen and Reza Adhami [6].

Em [6] a técnica proposta considera que os poros encontrados na pele podem ser modelados por uma função gaussiana em duas dimensões, um pouco modificada, dada pela equação (4.1), onde: x é a distância horizontal em *pixels* até o centro do poro, y é a distância vertical e $P(x, y)$ é o valor assumido para o modelo do poro.

$$P(x, y) = 1 - e^{-|x^2+y^2|^{\frac{1}{2}}} \quad (4.1)$$

O valor de $P(x, y)$ varia entre 0 e 1. O valor 0 correspondente ao centro do poro, ou seja, o fundo do poro. O valor 1 corresponde à superfície da pele. Contudo, na imagem capturada da impressão digital a escala de representação dos valores consiste em 256 níveis de cinza, onde o valor 0 corresponde à superfície da pele, ou seja, às cristas e o valor 255 corresponde aos vales.

Desta forma, para que o modelo do poro seja utilizável é necessário realizar duas transformações na imagem a ser inspecionada: inverter a escala de cinza e re-escalar os valores da imagem para o intervalo de zero a um. A expressão (4.2) é utilizada para realizar essas duas transformações.

$$F(x, y) = 1 - \frac{I(x, y)}{255} \quad (4.2)$$

As dimensões do modelo utilizado são uma decisão importante pois, quanto maior a área do modelo, mais dispendioso computacionalmente se torna. No entanto, um modelo de dimensões maiores também permite maior precisão na identificação dos poros. Em [6] defende-se que o modelo 3x3 é suficiente para a localização da maioria dos poros. Contudo, observou-se que com o modelo 3x3 boa parte dos poros contidos na imagem não foi localizada (ver seção 4.1.2). Por essa razão, decidiu-se avaliar o desempenho de modelos com dimensões maiores. Diversos testes foram realizados com modelos 3x3, 5x5 e 7x7 e o modelo 5x5 foi o que apresentou melhor resultado. O modelo 5x5 construído a partir da equação (4.1) é mostrado na Figura 4.4. A seção 4.1.1 apresenta detalhes das métricas utilizadas e dos testes realizados para a validação desta decisão.

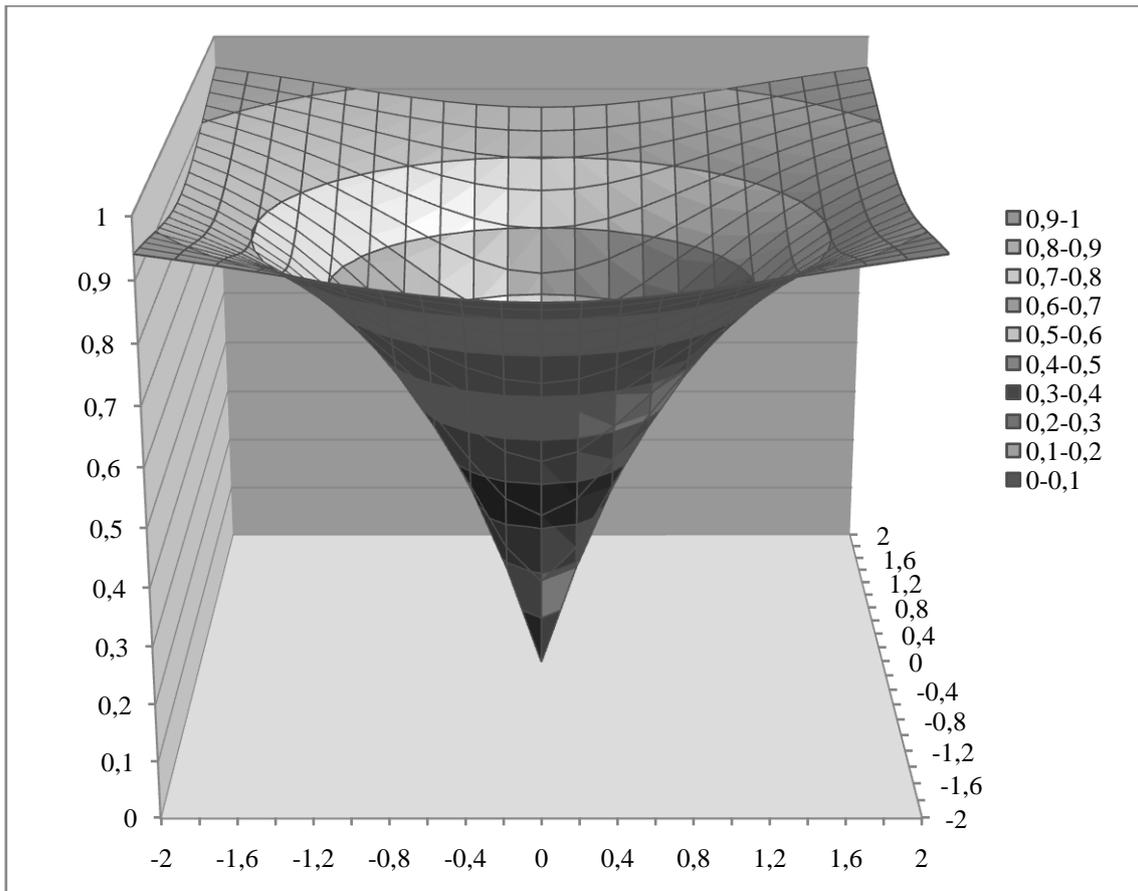


Figura 4.4 – Modelo utilizado para os poros da pele que aparecem na impressão digital.

Depois de definido o modelo para o poro e preparada a imagem, pode-se realizar a localização dos poros. Para isso, a imagem da impressão digital é varrida ponto a ponto e, para cada ponto o modelo, centrado nesse ponto, é verificado quanto à sua similaridade. A expressão utilizada para verificação da similaridade do modelo foi retirada de [6] e é mostrada na equação (4.3), onde $E(x, y)$ é o erro quadrático obtido na comparação entre modelo do poro, P , e a imagem ajustada, F ; e r é o raio do modelo.

$$E(x, y) = \sum_{i=x-r}^{x+r} \sum_{j=y-r}^{y+r} [F(i, j) - P(i - x + r, j - y + r)]^2 \quad (4.3)$$

A equação (4.3) retorna um mapa das áreas onde a probabilidade de existir poros é grande, ou seja, o mapa bidimensional dos erros quadráticos. Para facilitar a utilização deste mapa é interessante estabelecer um limiar máximo de erro a ser considerado. Esse limiar não é definido em [6], porém a equação (4.4) mostra a forma utilizada. Esta equação representa a diferença entre a média e o desvio padrão calculados para o mapa dos erros quadráticos. Essa maneira de estabelecer o limiar utilizado se mostrou eficiente, pois restringe de maneira eficaz as áreas onde a probabilidade de haver poros é alta.

$$\xi = \bar{E} - \frac{1}{w \cdot h} \sum_{x=1}^w \sum_{y=1}^h [E(x, y) - \bar{E}]^2 \quad (4.4)$$

Onde:

ξ é o limiar de máximo erro considerado;

\bar{E} é o erro médio;

w é a largura da imagem;

h é a altura da imagem.

Por fim, a localização dos poros é definida como sendo os pontos de mínimos locais pertencentes ao mapa de erros quadráticos. Para tanto, uma janela de inspeção do mapa de erros quadráticos é definida com o objetivo de limitar a vizinhança a ser considerada na inspeção desses pontos de mínimos locais. A janela utilizada para este trabalho foi de 5×5 pixels.

Depois de localizados, basta preencher os poros para que sua influência seja diminuída nas próximas etapas de processamento da impressão digital. Uma vez que [6]

não apresenta definição de como realizar este preenchimento, uma técnica foi proposta durante a confecção deste trabalho, qual seja: preencher a área do poro com o inverso do modelo re-escalado para o maior nível de cinza que a imagem original apresente. A expressão (4.5) foi utilizada para o modelo de preenchimento do poro e a Figura 4.5 ilustra a realização deste modelo.

$$PP(x,y) = \max(I) \cdot e^{-|x^2+y^2|^{\frac{1}{2}}} \quad (4.5)$$

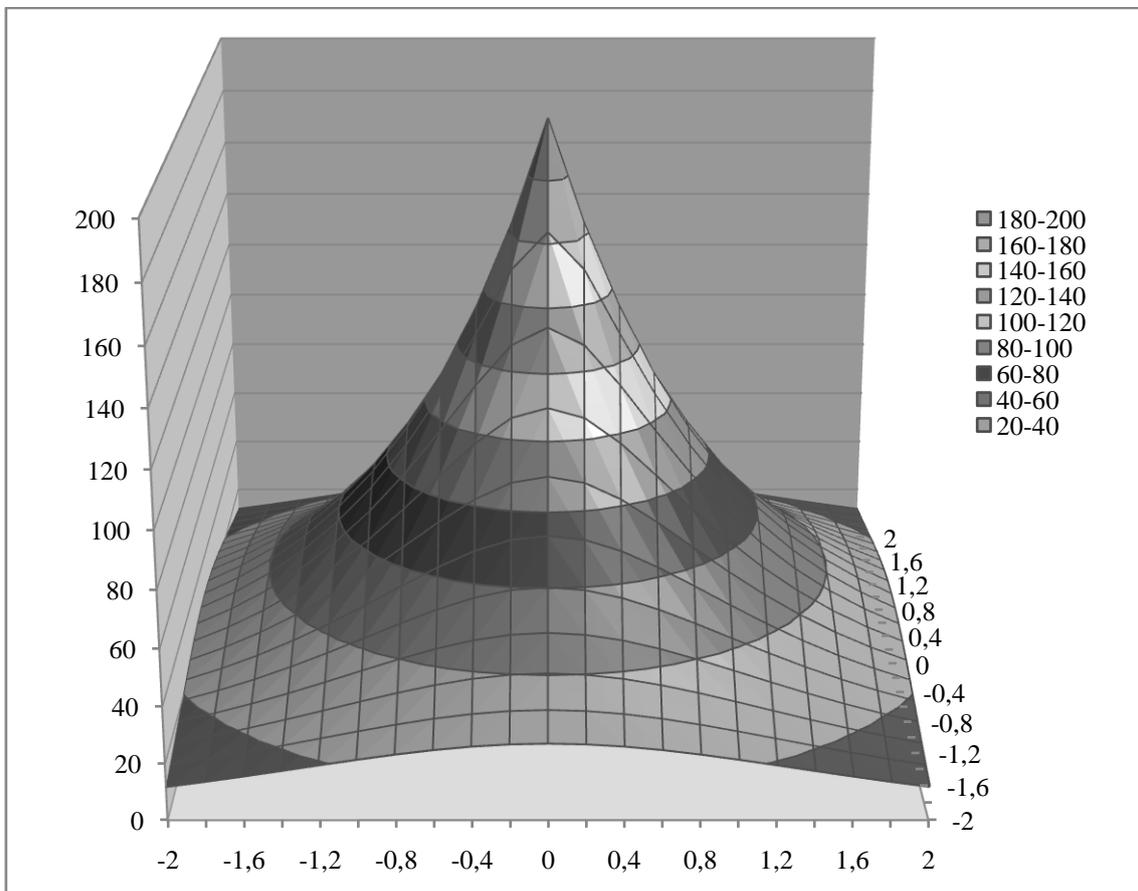


Figura 4.5 – Proposta de preenchimento do poro – considerando o maior nível de cinza da imagem da impressão digital original como sendo 255.

Dessa forma, a cada poro identificado na imagem original, soma-se o valor do modelo de preenchimento fazendo coincidir os pontos centrais do poro detectado e do preenchimento a ser aplicado. Contudo, o valor máximo resultante do preenchimento não deve suplantiar o valor máximo encontrado para a imagem como um todo, pois isso

pode afetar negativamente a precisão dos próximos passos do processamento da imagem. Assim, o modelo de preenchimento do poro é posicionado no local onde o poro foi detectado e somado ao poro, mas essa soma é limitada pela maior escala de cinza existente na imagem original. A Figura 4.6 ilustra o processo de detecção e preenchimento dos poros encontrados em uma imagem de impressão digital.



Figura 4.6 – Processo de identificação e extração de poros. Da esquerda para a direita, de cima para baixo: imagem original, mapa dos erros quadráticos, preenchimento para os poros detectados, imagem com os poros cobertos.

Para a avaliação da extração de poros, além da verificação da métrica de porcentagem de minúcias falsas, verificou-se que, para modelos de diferentes dimensões – 3x3, 5x5, 7x7 –, há diferentes proporções de número de poros verdadeiros encontrados na imagem e de pontos detectados como poros que, em verdade, não são. Dessa forma, estabeleceu-se a razão entre os poros verdadeiros e falsos encontrados e, ainda, entre as minúcias verdadeiras detectadas nas etapas posteriores do processamento e cada dimensão do modelo de poro.

4.1.1. Procedimento de teste

Inicialmente, para cada uma das impressões digitais do banco DB1 da FVC2004, foram extraídos e contados os poros. Esta contagem foi realizada automaticamente mas, para cada impressão digital, os poros falsos foram contados visualmente. Este procedimento foi realizado sobrepondo-se a imagem dos poros detectados e a imagem original da impressão digital. Dessa forma é possível identificar visualmente os poros detectados que não pertencem às linhas da impressão digital analisada.

Este procedimento introduz uma margem de erro causada pela imprecisão da inspeção humana para contagem dos poros falsos. Contudo, pode-se ver pela imagem de exemplo, mostrada na Figura 4.7, que não é difícil identificar os poros que não se encontram em uma linha da impressão digital, mas sim entre duas linhas. Em alguns casos a identificação da validade do poro fica difícil, e para estes casos, quando o poro não pode ser identificado claramente como verdadeiro, foi considerado falso. Vale ressaltar ainda que, durante o processo de contagem dos poros falsos, cerca de 5 % dos detectados não puderam ser classificados como verdadeiros ou falsos. Esta variação deve-se, na maioria dos casos, à má qualidade da imagem processada.

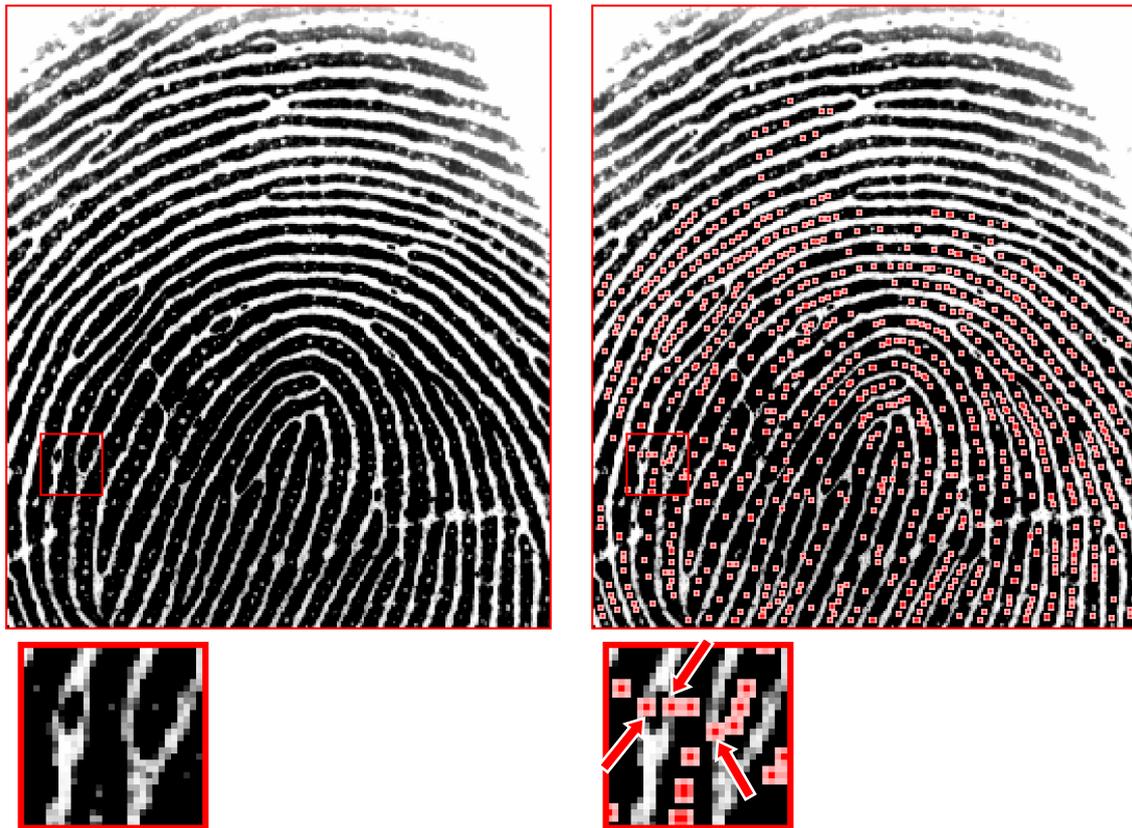


Figura 4.7 – Técnica utilizada para contagem de poros falsos. Na ampliação, os poros apontados são considerados falsos.

Por meio deste procedimento, foi possível medir a porcentagem de poros falsos no total de poros. Esta porcentagem foi medida para cada impressão digital do banco DB1 da FVC2004 e também para cada uma das dimensões escolhidas para o modelo do poro. A Tabela 4.1 mostra os resultados encontrados.

Tabela 4.1 – Medidas obtidas pela contagem de poros falsos.

Dimensões do modelo do poro (pixels)	Média de poros considerados falsos por imagem (porcentagem – quantidade)	Número médio de poros identificados automaticamente por imagem
3x3	3,94% – 12,2	309
5x5	2,53% – 9,5	374
7x7	2,89% – 11,2	386

Outra medida realizada, que se associa ao número de poros encontrados na imagem, foi o número de minúcias falsas encontradas ao final do processamento para cada dimensão do modelo de poro considerada. A Figura 4.8 mostra claramente que a

eliminação dos poros reduz drasticamente o número de minúcias falsas presentes na imagem afinada, obtida posteriormente. Contudo, para definir qual dimensão para o modelo de poro é mais conveniente, a Tabela 4.2 associa o número médio de minúcias falsas encontradas quando utilizada cada uma das dimensões. Este procedimento foi realizado concomitantemente à contagem de poros falsos. Para cada impressão digital do banco DB1 foram contadas as minúcias falsas encontradas ao final do processamento. O procedimento utilizado para a contagem de minúcias falsas está descrito mais à frente (seção 4.4.1).

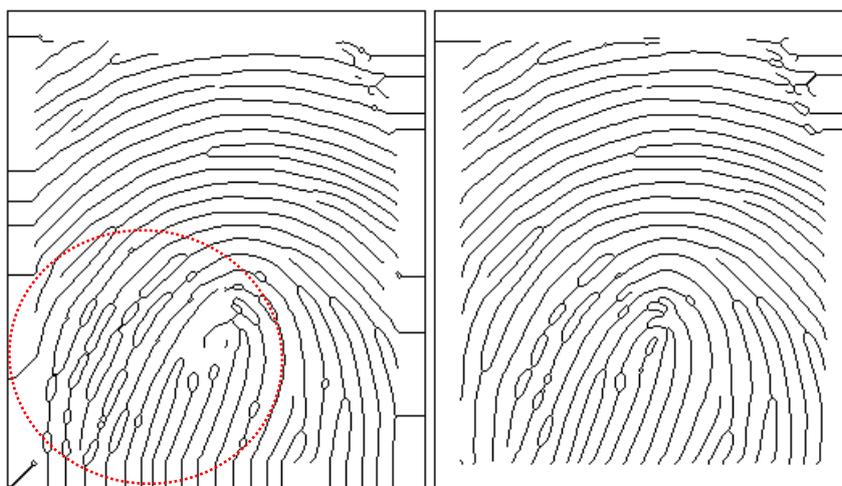


Figura 4.8 – Imagem afinada sem a extração de poros (esquerda) e com a extração de poros (direita).

Tabela 4.2 – Medidas relacionando dimensão do modelo de poro e número de minúcias falsas encontradas ao final do processamento.

Dimensões do modelo do poro (pixels)	Média de minúcias falsas encontradas por imagem (porcentagem – quantidade)	Número médio de minúcias encontradas automaticamente por imagem
3x3	23,8 % – 8,1	34
5x5	7,8 % – 2,2	28
7x7	11,3 % – 3,4	30

4.1.2. Análise dos resultados

A partir da Tabela 4.1 pode-se observar que o modelo de poro 3x3 identifica um número de poros substancialmente menor – cerca de 20 % a menos. O efeito desta diferença no número de minúcias falsas encontradas é facilmente identificado na Tabela

4.2: a diminuição do número de minúcias falsas é mais acentuada nos modelos 5x5 e 7x7.

Existe outro efeito observado por meio da Tabela 4.2: o número de minúcias encontradas após a utilização do modelo 7x7 aumenta quando comparado com o modelo 5x5. Esse fato foi investigado e observou-se que, como o modelo 7x7 possui uma área maior, quando o preenchimento do poro é realizado para os poros falsos, as linhas adjacentes a eles tendem a ser emendadas, e uma falsa minúcia de bifurcação se forma.

Assim, fica evidente que a extração de poros contribui bastante para a diminuição do número de minúcias falsas encontradas. Contudo, a dimensão do modelo mais interessante é a 5x5, pois, por meio dele o número de poros encontrados é maior do que pelo modelo 3x3, e o número de falsas minúcias inseridas pelo efeito de junção de linhas é menor.

4.2. DEFINIÇÃO DA ÁREA ÚTIL

Na grande maioria dos casos, as impressões digitais capturadas não cobrem por completo a imagem adquirida. Por essa razão, é comum a definição de algum parâmetro através do qual se determina qual é a parte da imagem que realmente contém informações úteis sobre a impressão digital capturada. Diversas técnicas podem ser consideradas (p.ex. [17] e [38]). Neste trabalho, duas técnicas foram utilizadas em conjunto, como já foi mencionado na seção 2.2.1.2.

A primeira técnica baseia-se no fato de que, em uma vizinhança suficientemente pequena, a variação dos tons de cinza encontrados na área útil de uma impressão digital é alta, pois há alternância quase regular entre máximos e mínimos. Por essa razão, o desvio padrão percebido para os valores de escala de cinza em uma região válida de uma impressão digital é alto. Pela mesma lógica, a região inválida da imagem – também chamada de região do fundo – apresenta baixo desvio padrão, pois apresenta, em sua maioria, valores de escala de cinza muito semelhantes entre si.

Essa técnica possui características interessantes tais como velocidade de processamento e precisão para encontrar regiões de fundo da imagem. Contudo, existe

um parâmetro a ser definido para a utilização deste método: a área da janela que define o setor a ser analisado para o cálculo do desvio padrão não pode ser muito grande nem muito pequena. Se essa área for muito grande, não se consegue definir setorialmente qual região da imagem é fundo ou não e, se for muito pequena, a chance de se encontrar um baixo desvio padrão aumenta, pois a variação aproximadamente senoidal entre os tons de cinza, que ocorre comumente na imagem da impressão digital, não aparece. Dessa forma, foram realizados testes com diversas áreas diferentes para esta janela e o valor que apresentou resultado mais preciso foi o de 16x16 pixels.

Contudo, notou-se ainda que o sentido em que a imagem é percorrida é determinante na definição da área considerada útil para a impressão digital. Por exemplo: se a imagem é inspecionada da direita para a esquerda, utilizando-se uma janela de 16 pixels de largura e a largura total da imagem não for múltipla de 16, ao final de cada linha de inspeção a janela fica truncada e, portanto, o efeito relativo a uma janela reduzida (descrito no parágrafo anterior) ocorre na borda esquerda da imagem – exemplo: Figura 4.9d.

Assim, a fim de eliminar o efeito de regiões do fundo que não foram detectadas pela razão descrita, realizou-se a inspeção da imagem em quatro sentidos: a) da esquerda para a direita e de cima para baixo; b) da esquerda para a direita e de baixo para cima; c) da direita para a esquerda e de cima para baixo; e d) da direita para a esquerda e de baixo para cima. Pode-se notar pela Figura 4.9 que a inspeção da esquerda para a direita (Figura 4.9a) complementa a inspeção realizada da direita para a esquerda (Figura 4.9b).

Dessa forma, observou-se que a superposição das quatro máscaras obtidas na inspeção em cada um dos quatros sentidos é claramente mais precisa e mais abrangente. O resultado final da utilização dessa técnica está exemplificado na Figura 4.9.

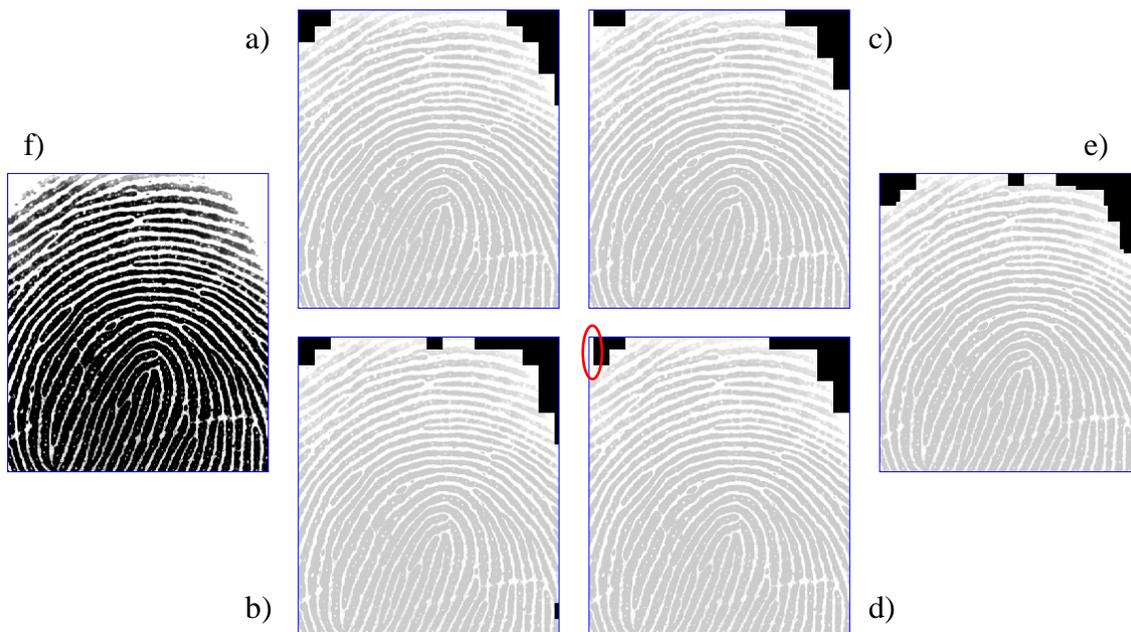


Figura 4.9 – Máscara de área útil definida por desvio padrão dos níveis de cinza. a) imagem original. Máscaras obtidas pela inspeção da impressão digital: b) da esquerda para a direita e de cima para baixo, c) da direita para a esquerda e de cima para baixo, d) da esquerda para a direita e de baixo para cima, e) da direita para a esquerda e de baixo para cima. f) máscara final.

A segunda consiste em verificar setorialmente se a frequência espacial das linhas da impressão digital está dentro de certa faixa. A frequência das linhas de impressões digitais para imagens com definição por volta de 500 dpi está entre $1/3$ e $1/25$ ([39] e [38]). Ou seja, as regiões onde a frequência se encontrar fora desta faixa possuem grande probabilidade de não serem área útil para as etapas subsequentes do processamento da imagem.

O cálculo do mapa de frequência para a imagem da impressão digital foi realizado segundo a técnica exposta em [7] (detalhes no Anexo B). Esta técnica produz um mapa de frequências ponto a ponto. Assim, a máscara de área útil apresenta o contorno mais bem definido, mas possui irregularidades nas regiões de fundo, como pode ser visto na Figura 4.10b. Por esta razão, uma seqüência de erosões e dilatações é realizada com o objetivo de tornar o contorno da máscara mais regular e de remover pequenas falhas que possam aparecer na região de fundo da máscara calculada. Primeiro, uma seqüência de 8 dilatações com raio de 1 pixel é realizada. Depois – Figura 4.10c –, são realizadas oito erosões com raio de 1 pixel. A Figura 4.10 ilustra o resultado da utilização desta técnica para a definição da máscara de área útil.



Figura 4.10 – Técnica de definição da área útil através do mapa frequencial. a) imagem da impressão digital, b) resultado da inspeção do mapa de frequências, c) dilatação da área útil, e d) erosão da área útil.

A técnica que utiliza o desvio padrão dos níveis de cinza é mais eficiente em detectar as regiões de fundo da imagem e a técnica de inspeção do mapa de frequências é mais eficiente em discernir as margens da imagem como um todo. Assim, para tornar a máscara de área útil mais robusta e abrangente, as duas técnicas descritas foram utilizadas em conjunto – Figura 4.11 – para gerá-la.



Figura 4.11 – União das duas técnicas de definição da área útil. Da esquerda para a direita: técnica de limiar do desvio padrão dos níveis de cinza, técnica de inspeção do mapa de frequências e sobreposição do resultado das duas técnicas.

Após a definição da área útil da imagem da impressão digital, as minúcias encontradas na região considerada inútil são descartadas. As minúcias localizadas na região de fundo ou em regiões de má qualidade da imagem devem ser, idealmente, escondidas pela máscara de área útil. Considerando-se que as minúcias encontradas nas regiões inválidas são sempre falsas ou, no mínimo, pouco confiáveis, este procedimento não elimina minúcias válidas.

4.2.1. Procedimento de teste

De acordo com a descrição realizada na seção 4.2, a área útil da imagem da impressão digital coletada foi definida por duas técnicas utilizadas em sobreposição. O procedimento de teste realizado teve por motivação confirmar a contribuição de cada técnica individualmente para a seleção da área útil final. Dessa forma, verificou-se o número de minúcias eliminadas do conjunto final para cada uma das técnicas individualmente e para a sobreposição das duas. A Tabela 4.3 mostra os resultados obtidos com este procedimento.

Tabela 4.3 – Resultados obtidos com a utilização das técnicas de definição da área útil.

Técnica de definição da área útil	Média de minúcias escondidas por imagem	Número médio de minúcias encontradas automaticamente após a utilização da máscara
Desvio Padrão dos tons de cinza	73	70
Inspeção da faixa de frequência local	32	111
Sobreposição das duas técnicas	93	50

Obs.: para o cálculo dos valores da última coluna levou-se em consideração o valor total de minúcias encontradas antes da utilização da máscara, que foi de 143 minúcias por imagem.

4.2.2. Análise dos resultados

Algumas conclusões podem ser retiradas dos valores registrados na Tabela 4.3. A primeira delas é que há sobreposição entre os conjuntos de minúcias escondidas por cada uma das técnicas isoladamente, pois, quando são utilizadas sobrepostas, seus resultados não são simplesmente somados – o que daria 105 e não 93. A segunda é que o número médio de minúcias eliminadas por ambas as técnicas por imagem é de 12. Essas conclusões podem ser verificadas por meio de um diagrama de Venn – Figura 4.12.

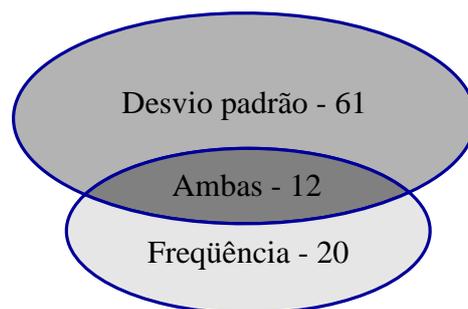


Figura 4.12 – Diagrama para análise do resultado da Tabela 4.3.

Dessa forma, o número de minúcias potencialmente espúrias eliminadas pela utilização das duas técnicas sobrepostas é maior do que o número eliminado individualmente por cada uma. Isso mostra que a sobreposição das duas técnicas é

efetiva e traz mais qualidade ao conjunto de informações biométricas extraído da imagem da impressão digital.

4.3. AFINAMENTO

Depois de realizada a melhoria e a binarização da imagem (seção 2.2.1.2), é necessário afinar as linhas detectadas na imagem da impressão digital. Este afinamento tem o objetivo de deixar as linhas com 1 pixel de largura. O trabalho [8] apresenta um estudo detalhado sobre o afinamento de linhas em imagens binarizadas – apenas dois tons distintos.

Idealmente, uma imagem afinada é formada pela linha central dos objetos que a constituem. Essa linha central é comumente chamada de esqueleto da imagem. O algoritmo de afinamento deve possuir algumas características básicas para ser considerado eficiente. Primeiramente, a conectividade dos objetos da imagem original deve ser mantida, ou seja, se dois objetos estão conectados na imagem original, seus esqueletos devem permanecer conectados na imagem afinada. Outra característica importante é que as proporções dos objetos em suas dimensões significativas não sejam diminuídas excessivamente, por exemplo: se uma linha deve ser afinada, sua largura deve ser reduzida ao máximo, mas o comprimento da linha deve permanecer o mais próximo possível do comprimento inicial.

Existem duas maneiras básicas de realizar o afinamento de imagens binarizadas: o afinamento serial – inspecionar a imagem e ir removendo os pontos detectados como bordas; ou o afinamento paralelo – inspecionar a imagem e marcar os pontos detectados como bordas para serem removidos na iteração seguinte. Ambas apresentam problemas.

A primeira técnica termina por identificar uma borda dos objetos afinados como sendo seu esqueleto, ou seja, o afinamento não é simétrico e depende do sentido de inspeção da imagem. Por exemplo, se a imagem é inspecionada linha a linha, da esquerda para a direita, e de baixo para cima a imagem afinada será formada pela borda inferior direita dos objetos que a constituem, pois os pontos superiores esquerdos serão removidos antes.

No afinamento paralelo, os pontos identificados como pertencentes às bordas dos objetos são marcados para serem removidos na iteração seguinte. Porém, se os pontos marcados não são utilizados para a análise da imagem na iteração corrente o formato dos objetos pode ser considerado erroneamente e, portanto, gerar distorções imprevistas do esqueleto. Por exemplo, uma linha de dois pixels de largura pode ser totalmente removida.

A técnica proposta em [8] consiste em utilizar tanto os pontos marcados quanto a imagem existente para decidir quais pontos eliminar, ou seja, para decidir quais pontos fazem parte das bordas da imagem, tanto os pixels marcados na iteração anterior quanto os pixels da imagem atual são utilizados. Desta maneira os problemas descritos são suplantados.

Em adição a essa idéia, o trabalho [8] propõe modelos de suavização das linhas finais da imagem. Esses modelos têm o objetivo de eliminar pontos que não são necessários para a estrutura dos objetos pertencentes à imagem original, mas que não são eliminados pela operação anterior.

Cada ponto da imagem afinada pertencente a algum objeto é comparado com os modelos de suavização. Se algum deles corresponder a um dos modelos, o ponto central pode ser eliminado sem prejuízo da conectividade e sem alterar a estrutura de formação do objeto de que faz parte.

Os modelos de suavização são formados por um ponto central e por seus 8 vizinhos imediatos. O ponto central deve pertencer a algum objeto – ou seja, não pode ser da região de fundo da imagem. Os pontos vizinhos devem estar em posições específicas como mostrado na Figura 4.13. Os pontos marcados com um “X” podem ser brancos ou pretos – respectivamente região de fundo ou objeto a ser afinado.

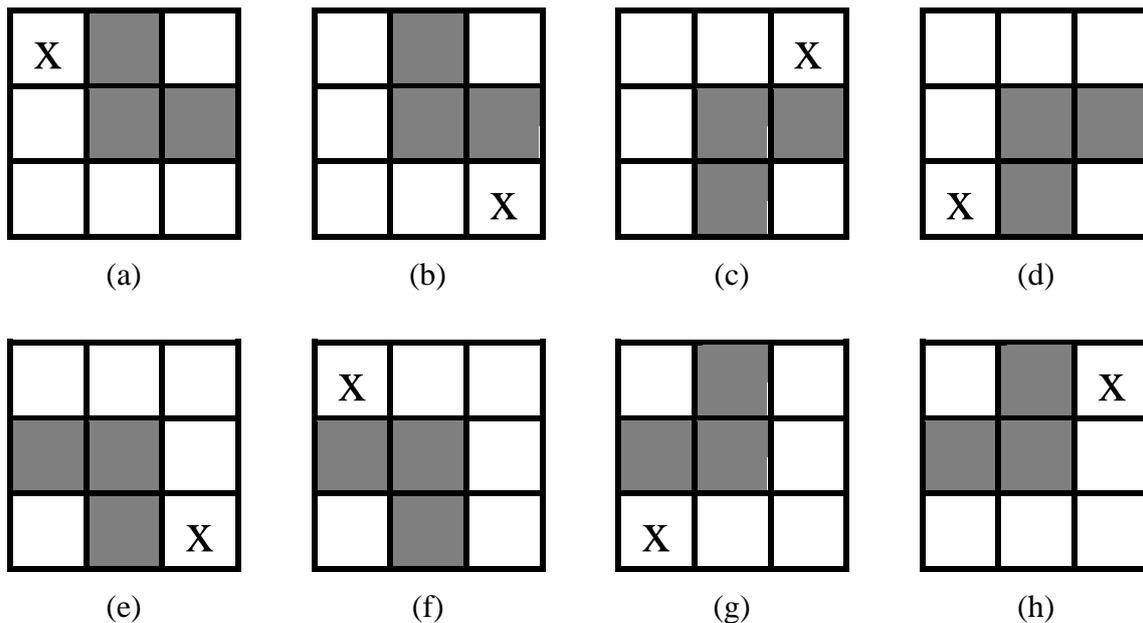


Figura 4.13 – Modelos de suavização (fonte: [8]).

Uma notação específica é definida para facilitar a descrição do algoritmo de afinamento. Uma representação para os pontos da imagem, outra para um mapa de marcações e três funções úteis são definidas para uso no algoritmo de afinamento. Os pontos da imagem a ser afinada utilizam a letra P . O mapa de marcações é utilizado em paralelo à imagem original para conter as marcações dos pontos a serem removidos na próxima iteração; logo, para cada ponto da imagem a ser afinada há um ponto no mapa de marcações. Os pontos do mapa de marcações utilizam a letra Q . As funções úteis são: $PN(P)$, $CN(P)$ e $Trans(P)$.

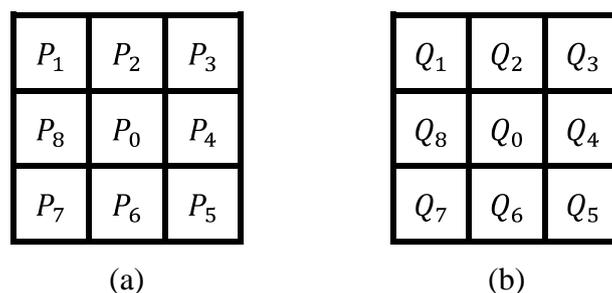


Figura 4.14 – a) Notação utilizada para o pixel a ser analisado, P_0 , e sua vizinhança, P_1 a P_8 . b) Notação utilizada para representar o mapa de marcações referente a P_0 .

Os valores assumidos por P e Q na notação definida na Figura 4.14 podem ser 0 ou 1. Para P , 1 simboliza um ponto do objeto a ser afinado e 0, um ponto de fundo. Para Q , 0 representa que o ponto está marcado para exclusão e 1, que não. Dessa forma define-se $PN(P)$, $CN(P)$ e $Trans(P)$ como:

$$PN(P_0) = \sum_{i=1}^8 P_i \quad (4.6)$$

$$CN(P_0) = \sum_{i=1}^8 (P_i \wedge Q_i) \quad (4.7)$$

$$Trans(P_0) = \sum_{i=1}^8 count(P_i) \quad (4.8)$$

onde:

$$count(P_i) = \begin{cases} 1, & \text{se } ((P_i \wedge Q_i) == 0) \wedge ((P_{i+1} \wedge Q_{i+1}) == 1) \\ 0, & \text{caso contrário} \end{cases}$$

com $P_9 = P_1, Q_9 = Q_1$

Dessa forma, o seguinte algoritmo é estabelecido:

Algoritmo 2 – Processo de afinamento.

Passo 1: para cada ponto P pertencente à imagem binarizada

- i) *contar PN(P), CN(P) e Trans(P);*
- ii) *se P for um ponto da borda que satisfaz o teste 1 e (o teste 2 ou o teste 3), marcar P para remoção;*

Os 3 testes são:

- teste 1: $(CN(P) > 1) \&\& (CN(P) < 6)$;
- teste 2: $(Trans(P) == 1)$;
- teste 3: *P e seus vizinhos se apresentam como um dos modelos da Figura 4.13;*

Passo 2: remover os pontos marcados;

Passo 3: repetir os passos 1 e 2 até que nenhum ponto possa ser removido.

Durante os testes do algoritmo Algoritmo 2 foram detectadas 4 novos modelos de suavização não contemplados em [8]. Estes modelos foram encontrados por causarem, em alguns casos, a detecção de uma falsa minúcia na etapa seguinte ao afinamento. É fácil notar que os modelos propostos aqui não são detectados como passíveis de exclusão pelo algoritmo utilizado, pois, para todos eles, se o mapa de marcações correspondente não possuir marcação prévia, tem-se $CN(P) = 3$ e $Trans(P) = 3$. Os modelos propostos estão representados na Figura 4.15.

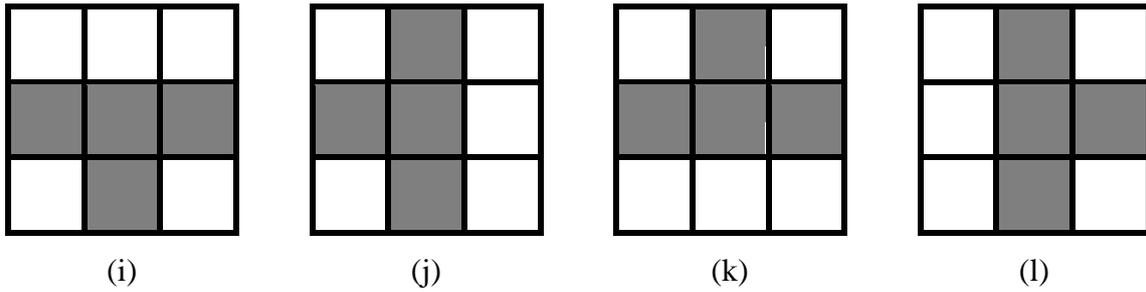


Figura 4.15 – Modelos de suavização propostos por este trabalho.

Removendo-se o pixel central dos modelos propostos na Figura 4.15 não há perda de conectividade e a medida de estreiteza (*thinness measuerment*) definida em [8] aumenta. A falsa minúcia desaparece após a utilização desses modelos de suavização, como pode ser verificado na Figura 4.16.

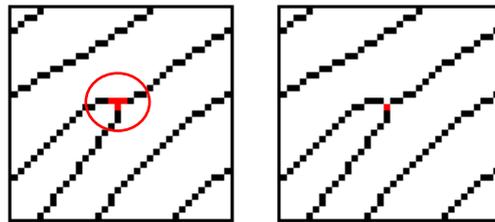


Figura 4.16 – exemplo de utilização de modelo de suavização. a) vários pontos classificáveis como bifurcação – ver seção 4.4; b) múltiplas minúcias eliminadas pela utilização do modelo de suavização da Figura 4.15i.

4.3.1. Procedimento de teste

A avaliação da técnica de afinamento construída foi realizada pela comparação com o resultado produzido pela técnica de afinamento utilizada em [7]. O afinamento também foi avaliado por meio do número de minúcias falsas detectadas após a utilização das técnicas em questão. A Tabela 4.4 apresenta os resultados obtidos.

A contagem de minúcias foi realizada por meio do procedimento descrito na seção 4.2.

Tabela 4.4 – Resultados obtidos após o processo de afinamento.

Técnica de afinamento	Média de minúcias falsas por imagem	Número médio de minúcias encontradas automaticamente após o afinamento
Proposta em [7]	12,2	38
Adaptada por este trabalho a partir de [8]	2,2	28

4.3.2. Análise dos resultados

Pode-se verificar por meio dos dados apresentados na Tabela 4.4 que o resultado obtido pelo algoritmo adaptado por este trabalho é significativamente superior ao algoritmo proposto em [7]. Isso se deve ao fato de que o este é menos rigoroso quanto à manutenção da conectividade das linhas afinadas, enquanto aquele restringe fortemente as regras de afinamento para garantir que a conectividade seja mantida. É trivial perceber que se uma linha antes contínua é segmentada pelo algoritmo de afinamento, novas minúcias poderão ser detectadas nos passos seguintes.

Cabe observar também, que a diferença entre o número médio de minúcias falsas encontradas por cada um dos métodos é idêntica à diferença entre o número médio total de minúcias encontradas automaticamente. O que também sinaliza o fato de que o algoritmo defendido em [7] acrescenta apenas minúcias falsas à impressão digital pela segmentação das linhas que a compõem.

4.4. LOCALIZAÇÃO E FILTRAGEM DAS MINÚCIAS

A partir das linhas afinadas da impressão digital, a localização das minúcias é um processo um tanto simples. As linhas da imagem são inspecionadas e, nos pontos onde houver descontinuidade pode haver uma minúcia. Essas descontinuidades podem ser detectadas por meio da análise dos pontos imediatamente vizinhos ao ponto investigado.

Para análise dos pontos imediatamente vizinhos, uma janela de 3 por 3 pixels é utilizada. Esta janela é centralizada em cada ponto pertencente às linhas afinadas

extraídas da imagem da impressão digital. Os vizinhos que fazem parte das linhas são contados e, caso não exista nenhum vizinho para o ponto analisado, trata-se de um ponto isolado, que deve ser ignorado. Se o ponto investigado possui apenas um vizinho, essa é considerada uma minúcia do tipo terminação. Se forem encontrados dois vizinhos para o ponto inspecionado, então não há descontinuidade na linha, e esse ponto deve ser desprezado. Se o ponto possui três (ou mais) vizinhos, então uma minúcia do tipo bifurcação deve ser registrada. A Figura 4.17 mostra exemplos dos casos descritos.

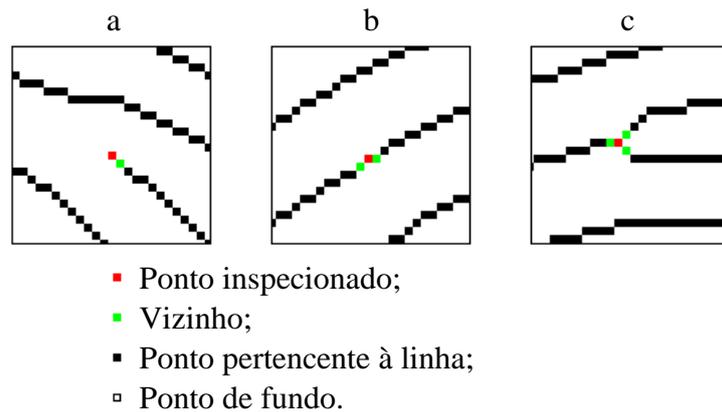


Figura 4.17 – Exemplos de pontos analisados para a localização de minúcias. a) 1 vizinho, minúcia de terminação b) dois vizinhos, ausência de descontinuidade c) 3 vizinhos, minúcia de bifurcação

Contudo, o ruído, presente nas etapas anteriores de processamento, pode criar terminações e bifurcações na imagem afinada que não correspondem às minúcias presentes na impressão digital original. Diversas técnicas podem ser utilizadas para tentar eliminar falsas minúcias do grupo das inicialmente detectadas por meio da inspeção da imagem afinada [40] [41].

Neste trabalho a técnica utilizada para eliminar minúcias consideradas falsas é baseada em [9], que consiste em acompanhar as linhas que contêm minúcias até a borda de uma janela de inspeção para verificar se a estrutura da linha que contém a minúcia está válida. Alguns exemplos de estruturas que contêm minúcias falsas são exibidos na Figura 4.18: para que uma minúcia seja verdadeira, a estrutura das linhas que a contêm, em uma vizinhança próxima, não deve seguir os casos aí ilustrados.

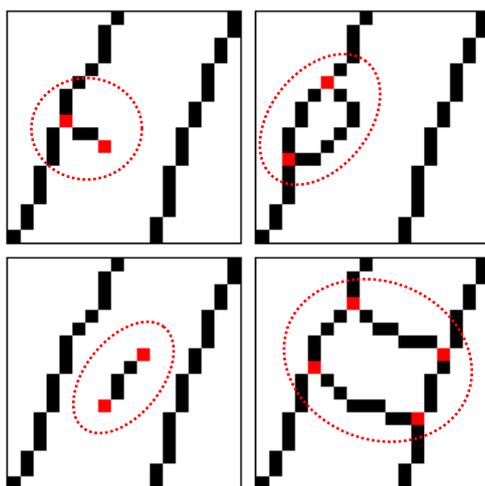


Figura 4.18 – Exemplos de estruturas que apresentam falsas minúcias (fonte: [9] com adaptações).

Verificou-se, ainda, durante a construção do software de teste, que o algoritmo defendido no trabalho de Marius Tico e Pauli Kuosmanen [9]) pode ser otimizado. O processo proposto por esses autores segue o seguinte algoritmo:

Algoritmo 3 – Processo de filtragem de minúcias proposto em [9]

Para cada minúcia localizada na imagem afinada:

- 1: *Criar uma imagem L de dimensões $W \times W$, inicializada com zeros, cujo centro coincide com a minúcia em análise, onde cada ponto de L corresponde a um ponto da imagem afinada.*
- 2: *Se a minúcia for do tipo terminação:*
 - a) *Preencher com o valor 1 os pixels de L que correspondam a pixels conectados à minúcia de terminação em análise;*
 - b) *Contar o número de transições de 0 para 1 (T_{01}) encontradas ao percorrer a borda de L no sentido horário;*
 - c) *Se $T_{01} = 1$, então a minúcia é válida; se não, é falsa.*
- 3: *Se a minúcia for do tipo bifurcação:*
 - a) *Percorrer, no sentido horário, os 8 vizinhos da minúcia analisada, preenchendo em L os pixels correspondentes aos pontos conectados à minúcia com 1, 2 e 3, à medida que forem encontrados.*
 - b) *Para cada $l = 1, 2, 3$, preencher com l todos os pontos de L que:*
 - i. *Estiverem preenchidos com 0;*
 - ii. *Estiverem conectados com um pixel de valor l ;*
 - iii. *Correspondam a um ponto de linha na imagem afinada;*
 - c) *Contar o número de transições de 0 a 1, 0 a 2 e 0 a 3 (T_{01}, T_{02}, T_{03}) encontradas quando a borda de L é percorrida no sentido horário.*
 - d) *Se $T_{01} = 1 \wedge T_{02} = 1 \wedge T_{03} = 1$, então a minúcia é verdadeira; se não, é falsa.*

Esse algoritmo é mais longo do que o necessário para verificar a unicidade das linhas que ligam a minúcia analisada às bordas da janela de inspeção (L), pois sempre analisa todos os pontos dentro da janela e ainda precisa percorrer, para todos os casos, a borda de L para verificar se o caminho é único ou não.

Foi criada uma alternativa de processamento que não necessita da verificação de todos os pontos da imagem e que, além disso, não necessita percorrer a borda da janela de inspeção. Este algoritmo encontra-se descrito abaixo:

Algoritmo 4 – Processo de filtragem de minúcias falsas proposto por este trabalho.

Para cada minúcia localizada na imagem afinada:

- 1: Criar uma imagem L de dimensões $W \times W$, inicializada com zeros, cujo centro coincide com a minúcia em análise, onde cada ponto de L corresponde a um ponto da imagem afinada.*
- 2: Se a minúcia for do tipo terminação:*
 - a) Sendo l_a o ponto de L em análise, inicializar l_a com o ponto relativo á minúcia inspecionada;*
 - b) Preencher l_a com o valor 1 (um);*
 - c) Se l_a for pertencente à borda de L , a minúcia é considerada verdadeira e o procedimento passa à próxima minúcia; caso contrário, passar ao passo seguinte;*
 - d) Verificar se, dentre os 8 vizinhos de l_a , existe algum ponto que seja relativo a uma linha na imagem afinada e que tenha valor 0 em L ;*
 - e) Se existir tal ponto, atribuir sua posição a l_a e voltar ao passo “2.b”; caso contrário, a minúcia é considerada falsa e o procedimento passa à próxima minúcia;*
- 3: Se a minúcia for do tipo bifurcação:*
 - a) Percorrer, no sentido horário, os 8 vizinhos da minúcia analisada, preenchendo com 1, 2, 3, etc. os pixels em L correspondentes aos pontos conectados à minúcia, à medida que forem sendo encontrados.*
 - b) Preencher o ponto de L relativo á minúcia com -1;*
 - c) Para cada $l = 1, 2, 3, \text{etc.}$:*
 - i. Posicionar l_a no ponto vizinho à minúcia preenchido com o valor de l ;*
 - ii. Se l_a for pertencente à borda de L , o procedimento passa ao próximo valor de l – passo “3.b”; caso contrário, passar ao passo seguinte;*
 - iii. Verificar se existe algum ponto que seja relativo a uma linha na imagem afinada e que tenha valor 0 em L , dentre os 8 vizinhos de l_a ;*
 - iv. Se existir tal ponto, atribuir a posição desse ponto a l_a , preenchê-lo com o valor de l , e voltar ao passo “3.c.ii”; caso contrário, a minúcia é considerada falsa e o procedimento passa à próxima minúcia;*

A Figura 4.19 mostra o funcionamento do algoritmo proposto para a validação de uma minúcia verdadeira e a Figura 4.20 ilustra a detecção de uma minúcia falsa.

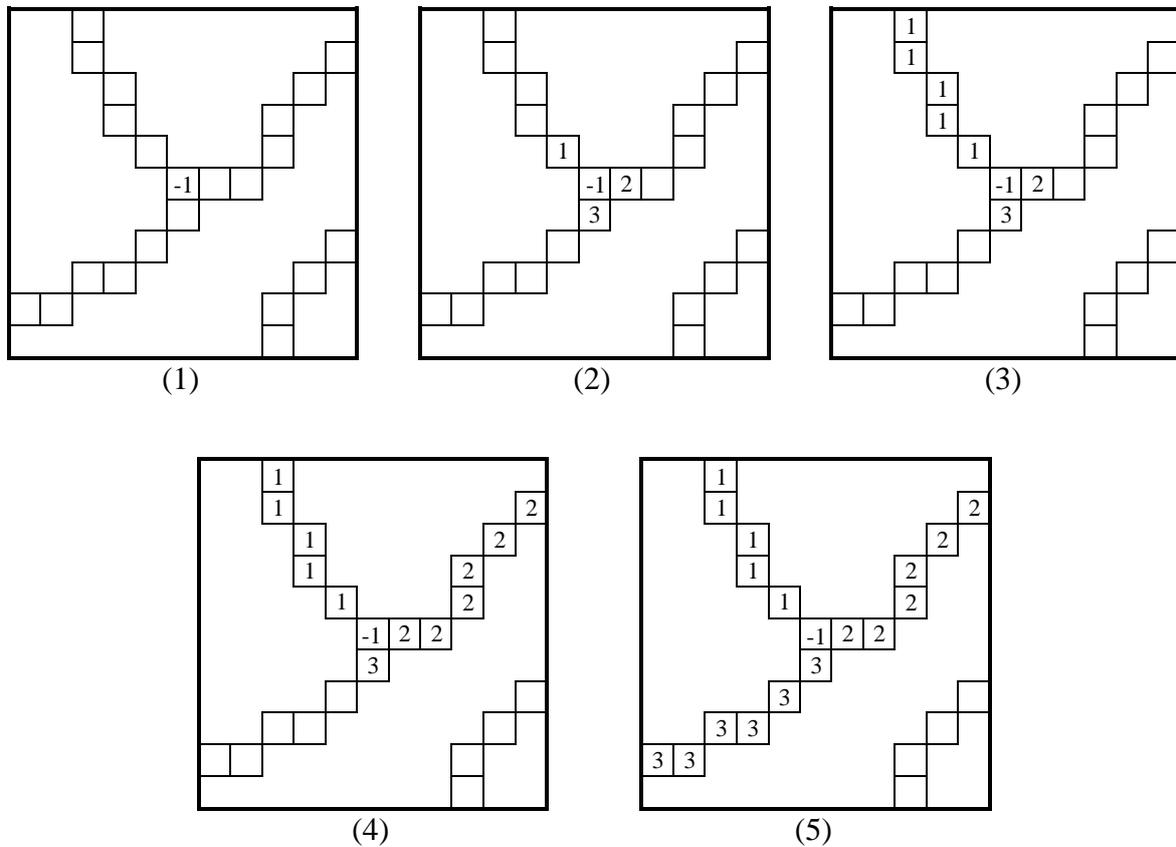


Figura 4.19 – Sequência de passos do algoritmo de detecção de falsas minúcias.

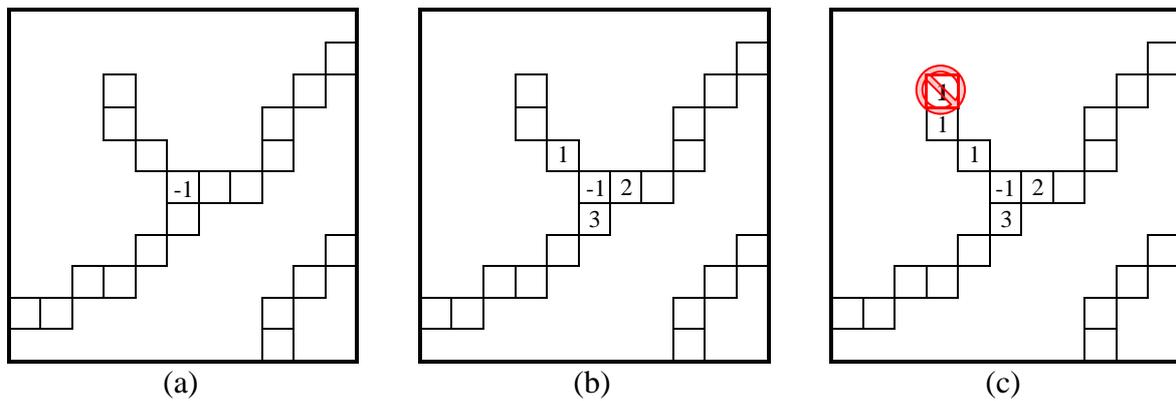


Figura 4.20 – Sequência de passos realizados para detectar uma minúcia do tipo bifurcação falsa.

O processo de filtragem das minúcias é o último passo do processamento para extrair a informação biométrica de uma imagem de impressão digital. Último mas não menos importante, pois, como foi descrito, este passo visa a eliminar eventuais minúcias

falsas que não tenham passado despercebidas ou até mesmo que tenham sido inseridas pelos processamentos anteriores.

4.4.1. Procedimento de teste

Para avaliar a eficiência da filtragem de minúcias utilizando o algoritmo alterado proposto na seção 4.4, o seguinte processo foi utilizado:

1. Contar o número de minúcias falsas obtidas até este ponto;
2. Utilizar o algoritmo de filtragem de minúcias proposto em [9], medindo o tempo gasto para realizar a filtragem e contar o número de minúcias falsas restantes;
3. Utilizar o algoritmo alterado proposto por este trabalho, também registrando o tempo de processamento gasto e contar o número de minúcias falsas restantes;
4. Tabela os dados obtidos acima para análise.

A contagem de minúcias citada no passo 1 acima foi realizada de forma semelhante à contagem de poros falsos mencionada na seção 4.1.1. As minúcias extraídas foram sobrepostas à imagem que lhes deu origem – como mostra a Figura 4.21 – e, visualmente, foram categorizadas como falsas as que não se encontravam em uma bifurcação ou uma terminação. Como o número total de minúcias já foi automaticamente obtido, o número de minúcias verdadeiras foi obtido subtraindo-se desse total a quantidade de minúcias identificadas como falsas. O número de minúcias total para os passos 1, 2 e 3 é obtido automaticamente, não sendo necessário contar todas as minúcias encontradas para todas as impressões digitais.

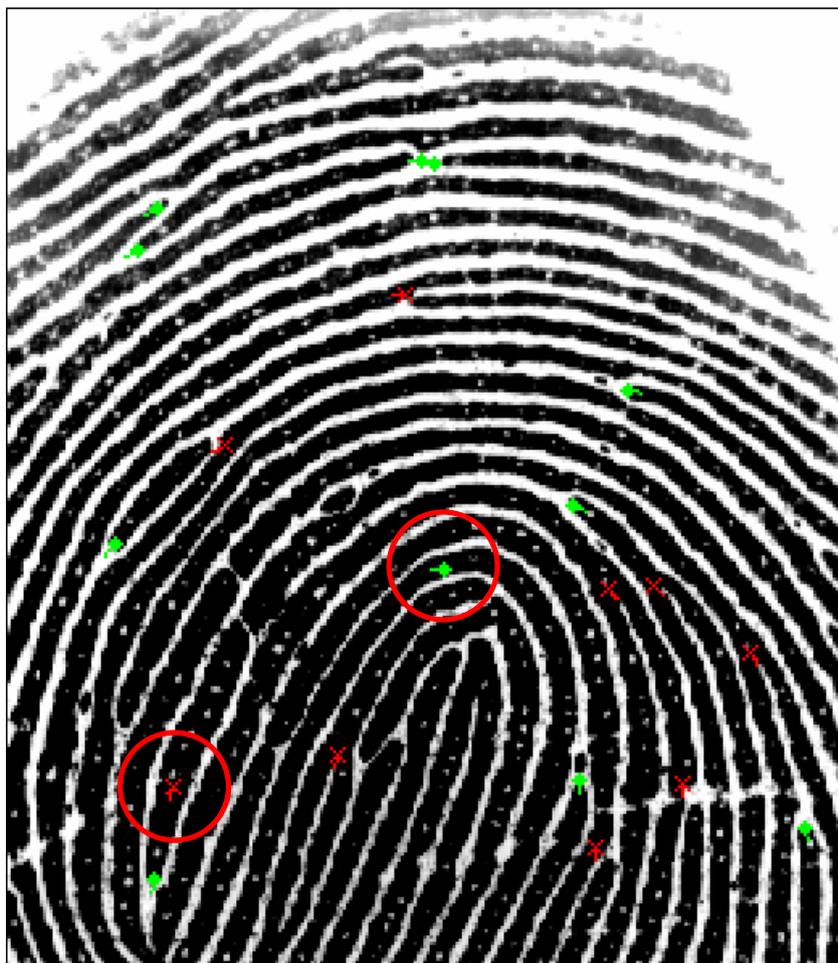


Figura 4.21 – Técnica utilizada para contagem das minúcias falsas obtidas ao final de todo o processamento: sobreposição da imagem original com as minúcias encontradas. As minúcias circuladas são consideradas falsas.

Vale ressaltar que é tarefa bastante mais simples e rápida a contagem de minúcias falsas do que a de poros falsos mencionada na seção 4.1.1, como mostra a Figura 4.21. A identificação de minúcias falsas pela sobreposição das minúcias encontradas ao final do processamento à imagem que as originou é direta. Dessa forma, a tabela a seguir sumariza as informações coletadas.

Tabela 4.5 – Resultados da filtragem de minúcias.

Algoritmo utilizado	Tempo médio gasto para filtrar as minúcias de uma imagem (milissegundos)	Número médio de minúcias falsas por imagem após a execução do algoritmo
Proposto em [9]	8,03	2,184
Adaptado por este trabalho	1,27	2,184

4.4.2. Análise dos resultados

A motivação para a adaptação do algoritmo de filtragem de minúcias proposto em [9], como foi dito anteriormente, é a de diminuir o tempo de processamento por meio da simplificação do processo. Pode-se notar, pelos dados contidos na Tabela 4.5, que o tempo de processamento para a filtragem de minúcias gasto pelo algoritmo proposto por este trabalho foi cerca de 84 % menor.

É possível notar ainda que o número de minúcias falsas encontradas após a utilização de ambos é exatamente o mesmo, o que não se trata de mera coincidência, mas sim da confirmação de que a adaptação do algoritmo filtrou as minúcias mais rapidamente sem alterar o número de minúcias falsas ao final do processamento, como era desejado.

4.5. ANÁLISE GERAL DOS RESULTADOS

Finalmente, depois de validados todos os passos da técnica utilizada para processar a imagem da impressão digital, é possível avaliar a qualidade da informação biométrica extraída. Foram definidas duas características para avaliar a qualidade dos dados biométricos: a porcentagem de minúcias falsas verificadas nos *templates* cadastrados e a organização – padronização e informações adicionais associadas – do banco de dados biométricos criado.

A qualidade de um banco de dados biométricos pode ser avaliada pela porcentagem de informação autêntica contida neste banco. Pelos valores contidos na Tabela 4.5, verifica-se que a porcentagem de informação confiável contida nos registros de minúcias armazenados no banco é de 92,2 %. Contudo, essa informação contempla todas as impressões digitais do banco DB1 da FVC2004, e uma parte das imagens contidas nesse banco tem qualidade muito baixa. Como descrito na seção 2.2.1.3, ao se utilizarem diversas amostras para cadastrar uma impressão digital, consegue-se eliminar boa parte das minúcias espúrias. Dessa forma foram utilizadas as quatro melhores amostras de cada dedo pertencente ao banco de dados DB1, e a porcentagem de minúcias verdadeiras subiu para 97,3 %.

Além disso, um banco de dados biométricos, para ter qualidade, deve ser utilizável de forma consistente e rápida pelas aplicações de identificação biométrica. Para isso, é necessário que a informação esteja bem organizada e categorizada. Por meio dos padrões internacionais expostos no Capítulo 3, criou-se um banco de dados de fácil acesso – pela padronização da interface de acesso, a BioAPI, e pelo padrão de formato de armazenamento ISO/IEC 19794-2 – e de utilização potencialmente rápida e eficiente, devido à classificação dos registros de minúcias.

Assim, pode-se verificar que a técnica utilizada para gerar um banco de dados biométricos de boa qualidade proposta por este trabalho obteve êxito nos quesitos mencionados. Contudo, existem alguns processos e características que ainda podem ser melhorados com o intuito de aumentar ainda mais a qualidade e usabilidade do banco de dados biométricos gerado. Esses processos e características serão comentados no capítulo seguinte como trabalho futuro.

5. CONCLUSÃO

Este trabalho visou a construir uma técnica de processamento de impressões digitais capaz de construir um banco de dados biométricos de impressões digitais de boa qualidade. Dois principais métodos foram utilizados para realizar esse objetivo: a pesquisa de trabalhos existentes seguida da escolha das técnicas mais modernas e eficientes, e da proposta de melhorias em algumas dessas técnicas para aprimorar os resultados obtidos. Existem, porém, diversos pontos que não foram abordados por este trabalho, mas que podem acrescentar ainda mais qualidade ao resultado final do processamento de impressões digitais para o cadastro de informações biométricas.

Uma pesquisa bibliográfica foi realizada durante a execução do presente trabalho. A consolidação dessas informações, que é um ganho secundário deste trabalho, reflete um pouco o estado da arte das técnicas de processamento de impressões digitais para aplicações de identificação biométrica. Contudo, o principal objetivo da pesquisa bibliográfica realizada foi o de escolher as técnicas que seriam utilizadas. Esse objetivo, por sua vez, foi cumprido, pois comparando-se trabalhos lidos foi possível identificar as técnicas mais pesquisadas e mais desenvolvidas atualmente para o processamento de informações biométricas de impressões digitais.

Depois de escolhidas as técnicas a serem utilizadas, este trabalho analisou detalhadamente cada uma e, com base nessa informação, propôs algumas melhorias em algumas delas. Além disso, um banco bem conhecido (DB1 da FVC2004) de imagens de impressões digitais foi utilizado para testar e validar a técnica proposta. Como as posições e números das minúcias verdadeiras para as impressões digitais desse banco não são conhecidas, diversas iterações de verificação visual dos resultados foram realizadas. Essas verificações foram facilitadas pelos procedimentos de teste estabelecidos no Capítulo 4. As estatísticas de minúcias falsas encontradas ao final do processamento foram utilizadas em vez das métricas mais usuais como curvas ROC, valores de FRR e de FAR. Isso foi feito porque o foco principal deste trabalho é na etapa de cadastro das impressões digitais e as métricas citadas são centradas na fase de verificação (*matching*) de sistemas de identificação biométrica.

Uma sugestão de um padrão de armazenamento da informação de classificação da impressão digital para complementar a ISO/IEC 19794-2 foi desenvolvida. O

formato criado se adéqua às especificações atuais da norma e apresentam flexibilidade para representar não apenas as classes utilizadas por este trabalho, mas um grande número de classes baseadas em diversos trabalhos relacionados à classificação.

Uma evolução da técnica de extração de poros proposta em [6] foi criada. O desempenho obtido em [6] foi melhorado e avaliado mais profundamente quanto à consequência de sua utilização. Diferentes dimensões para o modelo do poro foram testadas e, ao contrário do sugerido em [6], o modelo 5x5 foi considerado o de melhor resultado, tanto com relação à quantidade de poros encontrados – avaliação direta da técnica – quanto com relação à porcentagem de minúcias falsas encontradas ao final do processamento da impressão digital.

A utilização de duas técnicas sobrepostas para definição da área útil da imagem da impressão digital apresentou bons resultados. A qualidade do banco de dados biométricos de impressões digitais obtida com a utilização concomitante das duas técnicas foi superior à qualidade de qualquer das técnicas isoladamente. Apesar de haver uma área de redundância entre as técnicas utilizadas, a análise dos resultados obtidos mostra que é vantajoso utilizar a sobreposição das duas sob o ponto de vista da qualidade final do banco de dados biométricos.

Pequenas adaptações foram realizadas no processo de afinamento proposto em [8] por meio do acréscimo de quatro novos modelos de suavização da imagem afinada, possibilitando, assim, a utilização deste método de afinamento para o processamento de impressões digitais. O resultado final da técnica de afinamento foi comparado com o resultado obtido em [7] e mostrou vantagens quanto à quantidade de minúcias falsas detectadas ao final do processamento.

A criação de um algoritmo de filtragem das minúcias falsas equivalente ao proposto em [9], que apresenta tempo de processamento um tanto menor para realizar a filtragem de minúcias potencialmente falsas, é outra contribuição trazida por este trabalho. Que, no entanto, não teve o escopo realizar análise de desempenho computacional para a técnica desenvolvida.

Dessa forma, este trabalho desenvolveu uma técnica capaz de gerar um banco de dados biométricos de impressões digitais de boa qualidade. Como visto na seção 4.5, a quantidade de informação autêntica é alta – cerca de 97,3%.

As informações biométricas extraídas estão associadas a utilização de padrões internacionais – ISO/IEC 19794-2 e BioAPI – e também à classificação da impressão digital. Essas características, apesar de não serem diretamente mensuráveis, também constituem fatores de qualidade do banco de dados biométricos gerado. A BioAPI e a norma ISO/IEC 19794-2 dão às bibliotecas de funções biométricas criadas a característica de reusabilidade e interoperabilidade. E a classificação das impressões digitais cadastradas traz a possibilidade da utilização do banco de dados biométricos gerado para a identificação de grandes populações, pois acelera melhora o tempo de busca por uma impressão digital (identificação ou comparação 1:N) com base apenas na informação biométrica trazida pela candidata.

Algumas lacunas podem ser destacadas como possibilidades de trabalhos futuros que complementem a técnica desenvolvida aqui, sendo elas: estudo mais aprofundado de técnicas de melhoria da imagem da impressão digital equivalentes ao processamento realizado pelo filtro de Gabor; parametrização do algoritmo desenvolvido para processar imagens provenientes de diferentes tipos de sensores mantendo a eficiência global da técnica; pesquisa mais aprofundada e seleção de uma boa técnica de localização de pontos característicos – *cores* e deltas – das impressões digitais; associação desses pontos característicos aos dados do registro de minúcias para apoiar o processo de *matching* que utilize o banco gerado; avaliação de desempenho da técnica desenvolvida para verificar, sistematicamente, os tempos de processamento gastos por cada passo de processamento e o gasto de memória envolvido em cada etapa.

6. Referências Bibliográficas

- [1]. **Maltoni, D., D. Maio, A. K. Jain, and S. Prabhakar.** *Handbook of Fingerprint Recognition*. New York : Springer, 2003.
- [2]. **República Federativa do Brasil.** Lei nº 9.454 de 07 de Abril de 1997.
- [3]. **Silva, Yamar Aires da.** Estudo e proposta de um novo documento de identificação eletrônica (e-ID) para o Brasil. *Dissertação (mestrado) – Universidade de Brasília, Faculdade de Tecnologia, Departamento de engenharia Elétrica*. 2007. p. 147 f.
- [4]. **Campos, K. S. M. e Morais, H. M. C.** Sistema Único de Identificação. *Projeto Final de Graduação – Universidade de Brasília, Departamento de Engenharia Elétrica*. Agosto de 2006. p. 107 p.
- [5]. **Biometric System Lab - University of Bologna.** *FVC2004 - Fingerprint Verification Competition*. [Online] 2003. <http://bias.csr.unibo.it/fvc2004/>.
- [6]. **Michael Ray, Peter Meenen and Reza Adhami.** A Novel Approach to Fingerprint Pore Extraction. *Proceedings of the Thirty-Seventh Southeastern Symposium on System Theory*. 2005.
- [7]. **Patel, Shivang.** *FVS - Fingerprint Verification System*. [Online] 2003. <http://fvs.sourceforge.net/index.html>.
- [8]. **R. W. Zhou, C. Quek, G. S. Ng.** A Novel Single Pass Thinning Algorithm. *IEEE Transaction on System Man and Cybernetics*. 1994.
- [9]. **Tico, Marius e Kuosmanen, Pauli.** An Algorithm for Fingerprint Image Postprocessing. *Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers*. 2000.
- [10]. **Cappelli, Rafaele, et al.** Performance Evaluation of Fingerprint Verification Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006, Vol. 28.
- [11]. **Standardization, International Organization for.** ISO/IEC 19794-2. 2005.
- [12]. **BioAPI Consortium.** BioAPI Specification Version 1.1 . 16 de Março de 2001.
- [13]. **Henry, E. R.** *Classification and Uses of Fingerprints*. London : Routledge, 1900.
- [14]. **Tu Van Le, Ka Yeung Cheung, Minh Ha Nguyen.** A Fingerprint Recognizer Using Fuzzy Evolutionary Programming. *Proceedings of the 34th Hawaii International Conference on System Sciences*. 2001.
- [15]. **GUO, HAO.** A Hidden Markov Model Fingerprint Matching Approach. *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics*. 2005.
- [16]. **Marana, Aparecido Nilceu e Jain, Anil K.** Ridge-Based Fingerprint Matching Using Hough Transform. *Proceedings of the XVIII Brazilian Symposium on Computer Graphics and Image Processing*. 2005.
- [17]. **Chikkerur, Sharat e Ratha, Nalini.** Impact of Singular Point Detection on Fingerprint Matching Performance. *Fourth IEEE Workshop on Automatic Identification Advanced Technologies*. 2005.
- [18]. **He, Yuliang, et al.** Fingerprint Matching Based on Global Comprehensive Similarity. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006, Vol. 28.
- [19]. **Tai Pang Chen, Xudong Jiang and Wei Yun Yau.** Fingerprint Image Quality Analysis. *International Conference on Image Processing*. 2004.
- [20]. **Younhee Gil, Dosung Ahn, Sungbum Pan, Yongwha Chung.** Access Control System with High Level Security Using Fingerprints. *Proceedings of the 32nd Applied Imagery Pattern Recognition Workshop*. 2003.

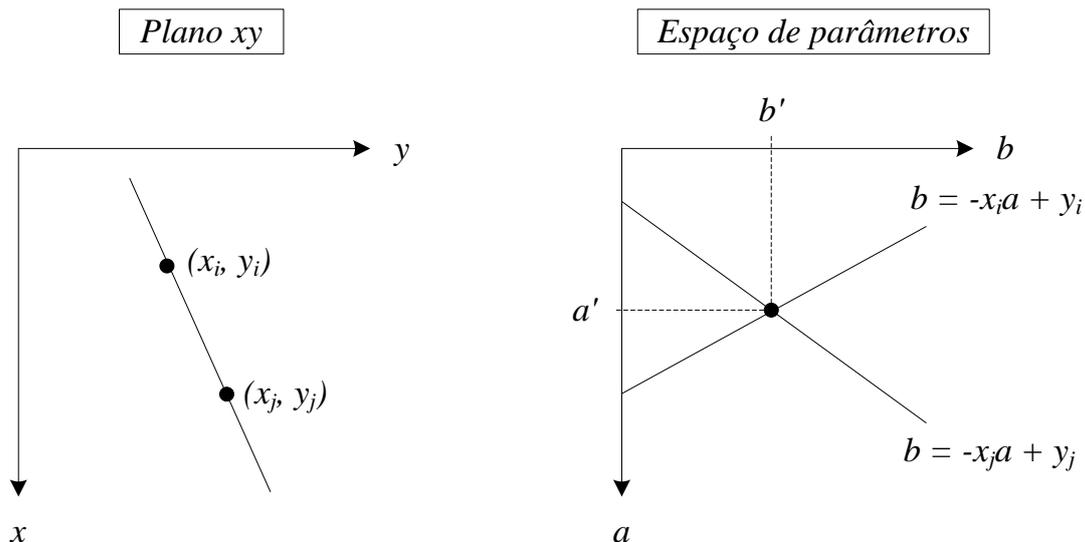
- [21]. **Biometric Systems Laboratory. BioLab.** [Online] DEIS - Department of Electronics, Computer sciences and Systems - University of Bologna. <http://biolab.csr.unibo.it>.
- [22]. **Guo, Hao, Ou, Zong-Ying e He, Yang.** Automatic Fingerprint Classification Based on Embedded Hidden Markov Models. *Proceedings of the Second International Conference on Machine Learning and Cybernetics*. Novembro de 2003.
- [23]. **Halici, Ugur e Ongun, Güçlü.** Fingerprint Classification Through Self-organizing Feature Maps Modified to Treat Uncertainties. *Proceedings of the IEEE*. 10 de Outubro de 1996, Vol. 84, pp. 1497 - 1512.
- [24]. **Jain, Anil K. e Minut, Silviu.** Hierarchical Kernel Fitting for Fingerprint Classification and Alignment. *Proceedings. 16th International Conference on Pattern Recognition*. 2002.
- [25]. **Jain, Anil K., Prabhakar, Salil e Hong, Lin.** A Multichannel Approach to Fingerprint Classification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. Abril de 1999, Vol. 21, pp. 348 - 359.
- [26]. **Krašnjak, Dubravko e Krivec, Vuk.** Fingerprint Classification Using a Homogeneity Structure of Fingerprint's Orientation Field and Neural Net. *Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis*. 2005.
- [27]. **Liu, Tong, et al.** Fingerprint Indexing Based on Singular Point Correlation. *IEEE International Conference on Image Processing*. 2005.
- [28]. **Senior, Andrew.** A Combination Fingerprint Classifier. *IEEE Transactions on Pattern Analysis And Machine Intelligence*. Outubro de 2001, Vol. 23, pp. 1165 - 1174.
- [29]. **Sha, Lifeng e Tang, Xiaoou.** Combining Exclusive and Continuous Fingerprint Classification. *International Conference on Image Processing*. 2004, pp. 1245 - 1248.
- [30]. **Wang, Sen, Zhang, Wei Wei e Wang, Yang Sheng.** Fingerprint Classification by Directional Fields. *Proceedings of the Fourth IEEE International Conference on Multimodal Interfaces*. 2002.
- [31]. **Cappelli, Raffaele, et al.** Fingerprint Classification by Directional Image Partitioning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. Maio de 1999, Vol. 21, pp. 402 - 421.
- [32]. **Maio, Dario e Maltoni, Davide.** A Structural Approach to Fingerprint Classification. *IEEE Proceedings of 13th International Conference on Pattern Recognition*. 1996, Vol. 3, pp. 578 - 585.
- [33]. **Ratha, Nalini K., et al.** A Real-time Matching System for Large Fingerprint Database. *IEEE Transactions PAMI*. 1996, pp. 799-813.
- [34]. **Consortium, BioAPI.** www.bioapi.org. *BioAPI Consortium*. [Online] 1998-2007.
- [35]. **Bhowmick, Partha e Bhattacharya, Bhargab B.** Approximate Fingerprint Matching Using Kd-tree. *Proceedings of the 17th International Conference on Pattern Recognition*. 2004.
- [36]. **Chan, K. C., Moon, Y. S. e Cheng, P. S.** Fast Fingerprint Verification Using Subregions of Fingerprint Images. *IEEE Transactions on Circuits and Systems for Video Technology*. janeiro de 2004, Vol. 14, pp. 95 - 101.
- [37]. **Sha, Lifeng, Tang, Xiaoou e Zhao, Feng.** Fingerprint Matching Using Minutiae and Interpolation-based Square Tessellation Fingercodes. *IEEE International Conference on Image Processing*. 2005.
- [38]. **Hong, Lin, Wan, Yifei e Jain, Anil.** Fingerprint Image Enhancement: Algorithm and Performance Evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1998, Vol. 20.

- [39]. **Jiang, Xudong.** A Study of Fingerprint Image Filtering. *Proceedings of the International Conference on Image Processing*. 2001, Vol. 3, pp. 238 - 241.
- [40]. **Ratha, N., Chen, S. e Jain, A.** Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images. *Pattern Recognition*. Novembro de 1995, Vol. 28, pp. 1657 - 1672.
- [41]. **Xiao, Q. e Raafat, H.** A Combined Statistical and Structural Approach for Fingerprint Image Postprocessing. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*. Novembro de 1990, pp. 331 - 335.
- [42]. **Gonzales, Rafael C. e Woods, Richard E.** *Digital Image Processing*. s.l. : Prentice Hall, 2003.
- [43]. **Ross, Arun, Dass, Sarat C. e Jain, Anil K.** Fingerprint Warping Using Ridge Curve Correspondences. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006, Vol. 28.
- [44]. **Wang, Yi, Hu, Jiankun e Schroder, Heiko.** A Gradient Based Weighted Averaging Method for Estimation of Fingerprint Orientation Fields. *Proceedings of the Digital Imaging Computing: Techniques and Applications*. 2005.
- [45]. **Parthasaradhi, Sujan T. V., et al.** Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices. *IEEE Transactions on Systems, Man, and Cybernetics — PART C: Applications and Reviews*. 2005, Vol. 35.
- [46]. **Wen, Miao-li, et al.** A Gabor Filter Based Fingerprint Enhancement Algorithm in Wavelet Domain. *IEEE International Symposium on Communications and Information Technology*. 2005, Vol. 2, pp. 1468 - 1471.
- [47]. **Jiang, Xudong.** On Orientation and Anisotropy Estimation for Online Fingerprint Authentication. *IEEE Transactions on Signal Processing*. 2005, Vol. 53.
- [48]. **Ma, Rui, et al.** A Novel Approach to Fingerprint Ridge Line Extraction. *IEEE International Symposium on Communications and Information Technology*. Outubro de 2005, Vol. 1, pp. 2 - 5.
- [49]. **Qi, Jin, et al.** A Novel Fingerprint Matching Method Based on the Hough Transform without Quantization of the Hough Space. *Proceedings of the Third International Conference on Image and Graphics*. 2004.
- [50]. **Moon, Y. S., et al.** Template synthesis and image mosaicking for fingerprint registration: an experimental study. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*. 2004, Vol. 5.
- [51]. **Ng, G. S., et al.** Adjacent Orientation Vector Based Fingerprint Minutiae Matching System. *Proceedings of the 17th International Conference on Pattern Recognition*. 2004.
- [52]. **Nagaty, K. A.** An Energy-Based Fingerprint Matching System. *Consumer Communications and Networking Conference*. 2004, pp. 706 - 709.
- [53]. **Jia, Congzhi, Xie, Mei e Li, Qingrong.** A Fingerprint Minutiae Matching Approach Based on Vector Triangle Method and Ridge Structure. *International Conference on Communications, Circuits and Systems*. 2004, Vol. 2, pp. 871 - 875.
- [54]. **Wu, Chenyu, et al.** Robust Crease Detection in Fingerprint Images. *Proceedings of the 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. 2003.
- [55]. **Simon-Zorita, D., et al.** Image quality and position variability assessment in minutiae-based fingerprint verification. *IEEE Proceedings on Vision, Image and Signal Processing*. 2003.
- [56]. **Tan, Xuejun e Bhanu, Bir.** On The Fundamental Performance For Fingerprint Matching. *Proceedings of the 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. 2003.

- [57]. **Yang, Shenglin, Sakiyama, Kazuo e Verbauwhede, Ingrid M.** A Compact and Efficient Fingerprint Verification System for Secure Embedded Devices. *Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers*. 2003.
- [58]. **Omnia, Vesa e Tico, Marius.** Adaptive Binarization Method For Fingerprint Images. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*. 2002.
- [59]. **Zhang, Weiwei e Wang, Yangsheng.** Core-Based Structure Matching Algorithm of Fingerprint Verification. *Proceedings of the 16th International Conference on Pattern Recognition*. 2002.
- [60]. **Ko, Teddy.** Fingerprint Enhancement by Spectral Analysis Techniques. *Proceedings of the 31st Applied Imagery Pattern Recognition Workshop*. 2002.
- [61]. **Ikeda, Namiko, et al.** Fingerprint Image Enhancement by Pixel-Parallel Processing. *Proceedings of the 16th International Conference on Pattern Recognition*. 2002, Vol. 3.
- [62]. **Rämö, Pauli, et al.** Optimized Singular Point Detection Algorithm for Fingerprint Images. *Proceedings of the International Conference on Image Processing*. 2001, Vol. 3, pp. 242 - 245.
- [63]. **Kovács-Vajna, Zsolt Miklós.** A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2000, Vol. 22, pp. 1266 - 1276.
- [64]. **Ghosal, Sugata, et al.** Hierarchical Partitioned Least Squares Filter-Bank for Fingerprint Enhancement. *Proceedings of the 15th International Conference on Pattern Recognition*. 2000, Vol. 3, pp. 334 - 337.
- [65]. **Ratha, Nalini K., et al.** Robust Fingerprint Authentication Using Local Structural Similarity. *Fifth IEEE Workshop on Applications of Computer Vision*. 2000, pp. 29 - 34.
- [66]. **Ghosal, Sugata, et al.** Learning Partitioned Least Squares Filters for Fingerprint Enhancement. *Fifth IEEE Workshop on Applications of Computer Vision*. 2000, pp. 2 - 7.
- [67]. **Jain, Anil, Hong, Lin e Bolle, Ruud.** On-Line Fingerprint Verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. abril de 1997, Vol. 19, pp. 302 - 314.

ANEXO A – TRANSFORMADA DE HOUGH [42]

Considere um ponto (x_i, y_i) e a equação geral da reta na forma inclinação-interceptação, $y_i = ax_i + b$. Infinitas linhas cruzam esse ponto, mas todas elas satisfazem a equação dada, apenas variando os valores de a e b . Contudo, reescrevendo a equação como $b = -x_i a + y_i$, e considerando o plano “ ab ” (também chamado espaço de parâmetros), uma linha é definida para o par fixo (x_i, y_i) . Além disso, um segundo ponto (x_j, y_j) também está associado uma linha no espaço de parâmetros, e essa linha intersecta a linha associada a (x_i, y_i) em (a', b') , onde a' é a inclinação e b' é a interseção da linha que contém tanto (x_i, y_i) quanto (x_j, y_j) no plano “ xy ”. A figura abaixo ilustra esses conceitos.



Um problema de utilizar a equação $y = ax + b$ para representar a reta é que a inclinação, “ a ”, se aproxima de infinito quando a reta se aproxima da vertical. Uma maneira de contornar esta dificuldade é usar a representação normal da reta:

$$x \cos \theta + y \sin \theta = \rho$$

A mesma transformação pode ser realizada, mas o espaço de parâmetros apresentará, para cada ponto (x, y) , uma curva senóide no plano “ $\theta\rho$ ”.

Dessa mesma forma, as transformações de Hough podem ser generalizadas para qualquer função da forma $g(\mathbf{v}, \mathbf{c}) = 0$, onde \mathbf{v} é um vetor de coordenadas e \mathbf{c} é um vetor de coeficientes. Por exemplo, os pontos que fazem parte do círculo:

$$(x - c_1)^2 + (y - c_2)^2 = c_3^2$$

ANEXO B – CÁLCULO DO MAPA DE FREQUÊNCIAS [7]

Neste passo a frequência das linhas da impressão digital é estimada. Em uma vizinhança local onde não aparecem minúcias ou pontos singulares (*cores* ou deltas), os níveis de cinza no sentido transversal às linhas e vales – normal à direção contida no mapa de orientação – podem ser modelados por uma onda de forma senoidal. Assim, a frequência local das linhas é propriedade intrínseca de uma impressão digital.

Sendo G a imagem normalizada de uma impressão digital, e O o mapa de orientação das linhas dessa imagem, os passos envolvidos na estimação da frequência local são os seguintes:

- 1 – Dividir G em blocos de $w \times w$ (16×16);
- 2 – para cada bloco com centro no pixel (i, j) , computar a janela orientada de tamanho $l \times w$ (32×16) que é definida no sistema de coordenadas alinhado às linhas da impressão digital;
- 3 – Para cada bloco com centro no pixel (i, j) , computar as “*x-signatures*” $X[0], X[1], \dots, X[l-1]$ das linhas e vales dentro da janela orientada, onde:

$$X[k] = \frac{1}{w} \sum_{d=0}^{w-1} G(u, v), \quad k = 0, 1, \dots, l-1$$

$$u = i + \left(d - \frac{w}{2}\right) \cdot \cos O(i, j) + \left(k - \frac{l}{2}\right) \cdot \sin O(i, j)$$

$$v = j + \left(d - \frac{w}{2}\right) \cdot \sin O(i, j) + \left(k - \frac{l}{2}\right) \cdot \cos O(i, j)$$

Se nenhuma minúcia e ponto singular aparecem na janela orientada, $X[k]$ forma uma onda discreta de formato senoidal, a qual possui a mesma frequência das linhas e vales na janela orientada. Dessa forma, a frequência de linhas e vales pode ser estimada a partir de $X[k]$.

Sendo $T(i, j)$ o número médio de pixels entre dois picos consecutivos em $X[k]$, então a frequência, $OHM(i, j)$, é computada como:

$$OHM(i, j) = \frac{1}{T(i, j)}$$

Se não é possível detectar picos consecutivos em $X[k]$, então a frequência para este ponto recebe o valor -1, para diferenciá-la dos valores válidos de frequência;

- 4 – Para uma imagem capturada com resolução fixa, o valor da frequência de linhas e vales em uma vizinhança local cai em certa faixa. Para uma imagem de 500 dpi, por exemplo, esta faixa é entre $1/3$ e $1/25$. Logo, se a frequência estimada está fora desta faixa, o mapa de frequências recebe, para este ponto, o valor -1 para indicar que um valor válido de frequência não pode ser definido.