UNIVERSIDADE ESTADUAL PAULISTA
"Júlio de Mesquita Filho"
Pós-Graduação em Ciência da Computação

Murilo Varges da Silva

Detecção de Impressões Digitais Falsas no Reconhecimento Biométrico de Pessoas

BAURU

2015

Murilo Varges da Silva

Detecção de Impressões Digitais Falsas no Reconhecimento Biométrico de Pessoas

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação - Área de Concentração em Computação Aplicada, linha de Processamento de Imagens e Visão Computacional, como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Aparecido Nilceu Marana

Co-orientadora: Profa. Dra. Alessandra Aparecida Paulino

BAURU

2015

Silva, Murilo Varges da.
Detecção de impressões digitais falsas no reconhecimento biométrico de pessoas / Murilo Varges da Silva. -- São José do Rio Preto, 2015
99 f. : il., gráfs., tabs.

Orientador: Aparecido Nilceu Marana
Coorientador: Alessandra Aparecida Paulino
Dissertação (mestrado) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas

1. Computação. 2. Sistemas de detecção de intrusão (Medidas de segurança) 3. Biometria. 4. Datiloscopia. I. Marana, Aparecido Nilceu. II. Paulino, Alessandra Aparecida. III. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. IV. Título.

CDU – 681.3.025

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Murilo Varges da Silva

Detecção de Impressões Digitais Falsas no Reconhecimento Biométrico de Pessoas

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação - Área de Concentração em Computação Aplicada, linha de Processamento de Imagens e Visão Computacional, como parte dos requisitos para obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

Prof. Dr. Aparecido Nilceu Marana
Professor Adjunto
UNESP - Bauru
Orientador

Prof. Dr. Maurilio Boaventura
Professor Adjunto
UNESP – S. J. Rio Preto

Prof. Dr. Neucimar Jerônimo Leite
Professor Associado
UNICAMP - Instituto de Computação

BAURU, 31 de Julho de 2015.

Aos meus pais, Luiz e Luzinete.

Agradecimentos

Agradeço primeiramente a Deus pelo dom da vida e pela graça de concluir mais esta etapa em minha história acadêmica.

Ao meu orientador, Prof. Dr. Aparecido Nilceu Marana, pela grande confiança e envolvimento na condução deste trabalho, fundamentais para superação dos obstáculos que surgiram. Sua dedicação, reflexões e atenção aos detalhes foram inspiração à minha pesquisa e vida pessoal.

À minha co-orientadora Dra. Alessandra Aparecida Paulino, pela grande contribuição na definição dos objetivos e pelas sugestões e correções no desenvolvimento deste trabalho.

Aos meus pais Luiz e Luzinete, e minhas irmãs Fabiana, Mônica e Priscila, pelo exemplo, pela motivação, educação, carinho e apoio incondicional, com os quais compartilho todos os meus sonhos e conquistas.

À minha esposa Priscila Anjos pelo apoio incondicional, motivação e compreensão, com a qual compartilho esta conquista.

À minha família e amigos, pelo grande apoio e compreensão nos momentos em que estive ausente, pelos quais tenho profunda admiração e gratidão por fazerem parte de minha vida.

Ao IFSP, por incentivar e entender a importância do título de mestrado, e me conceder incentivo e o afastamento no último ano do curso.

Ao grupo de pesquisa RECOGNA da UNESP Bauru pelas valiosas discussões em nossos seminários semanais, que nortearam o andamento desta pesquisa.

E por fim, à UNESP, pela infraestrutura oferecida e pela qualidade do Programa de Pós-Graduação em Ciência da Computação.

"É muito melhor lançar-se em busca de conquistas grandiosas,
mesmo expondo-se ao fracasso,
do que alinhar-se com os pobres de espírito,
que nem gozam muito nem sofrem muito,
porque vivem numa penumbra cinzenta,
onde não conhecem nem vitória, nem derrota."
(Theodore Roosevelt)

Resumo

Nos últimos anos, diversas características biométricas têm sido propostas para a identificação de pessoas, dentre as quais destacam-se a face, a íris, a retina, a geometria da mão. Entretanto, a impressão digital ainda é a característica mais utilizada, tanto em aplicações comerciais quanto governamentais. Dentre as principais aplicações que utilizam impressões digitais podemos citar a identificação de eleitores por meio de urnas eletrônicas biométricas, o controle de fronteiras e imigração por meio dos passaportes, o acesso aos serviços bancários por meio de caixas bancários eletrônicos biométricos, entre outros. Com o aumento da utilização destes sistemas, as tentativas de ataque também aumentam. Dentre os tipos de ataques que um sistema biométrico baseado em impressões digitais pode sofrer, a apresentação de um dedo falso ao sensor é a técnica mais utilizada por pessoas mal intencionadas. Este trabalho tem como objetivo propor um método robusto para detecção de impressões digitais falsas, por meio da incorporação de informações dos poros sudoríparos. O método proposto foi avaliado utilizando-se uma base de dados própria denominada UNESP *Fingerprint Spoof Database* (UNESP-FSDB). A análise considerou alguns fatores que podem influenciar na detecção de impressões digitais falsas, tais como: (i) resolução da imagem da impressão digital; (ii) utilização de características de terceiro nível (poros); (iii) pressão do dedo sobre a superfície do sensor; (iv) tempo de aquisição da imagem da impressão digital; (v) umidade presente no dedo no momento da captura da impressão digital. Os resultados dos experimentos realizados mostraram que: (i) a utilização de informações de poros pode aumentar a acurácia em até 9%; (ii) a aplicação de uma maior pressão contra o sensor no momento da captura melhora a performance; (iii) a umidade presente no dedo influencia na qualidade da imagem e tem reflexos também na acurácia da detecção de impressões digitais falsas.

Palavras-chave: *Biometria, Segurança, Impressão Digital Falsa, Características de Terceiro Nível, Poros.*

Abstract

In recent years, many biometrics traits have been proposed to biometric identification of people, among which stand out the face, iris, retina, hand geometry. However, fingerprint is still the most used feature in both commercial and government applications. The main applications we can mention are the identification of voters through electronic voting machines, border control and immigration through passports, access to banking services through biometric *Automated Teller Machine* (ATM), among others. With the increased use of these systems, attempts to attack also increase. Among the types of attacks that a biometric system based on fingerprint may suffer, presenting a false finger to the sensor is the most used technique by malicious people. This work aims to propose a robust method to detect fake fingerprints by incorporating information from the sweat pores. The proposed method was assessed on own database named UNESP *Fingerprint Spoof Database* (UNESP-FSDB), the analysis considered some factors that may influence method performance as: (i) fingerprint image resolution ; (ii) use of third-level characteristics (pores); (iii) finger pressure on the sensor surface; (iv) fingerprint image acquisition time; (v) finger moisture present in the moment of capture fingerprint. The results of the experiments showed that: (i) incorporating information of pores can increase the accuracy up to 9%; (ii) using increased pressure at the time of capture improves the performance; (iii) the moisture present in the finger can influence the image quality and accuracy of the proposed method.

Key-words: *Biometrics, Security, Fingerprint Spoof, Third Level Fingerprint Features, Pores.*

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

ATM	*Automated Teller Machine.* vi
DAPM	*Dynamic Anisotropic Pore Model.* 65, 66
DNA	*Ácido Desoxirribonucleico.* 7
DoG	*Difference of Gaussian.* 65, 66
DoS	*Denial of Service.* 26
dpi	*Dots per Inch.* 15, 17
ED	*Euclidean Distance.* 41
EER	*Equal Error Rate.* 22, 30, 38
FAR	*False Acceptance Rate.* 21–23, 30
FBI	*Federal Bureau of Investigation.* 17
FDR	*False Detection Rate.* 63, 67, 68, 70, 71
FMR	*False Match Rate.* 21
FNMR	*False Non-Match Rate.* 21
FRR	*False Rejection Rate.* 21–23, 30
FTIR	*Frustrated Total Internal Reflection.* 11, 13, 17, 18
FVC	*Fingerprint Verification Competition.* 85
IAFIS	*Integrated Automated Fingerprint Identification System.* 16
IAFIS IQS	*Integrated Automated Fingerprint Identification System Image Quality Specification.* 16, 17
IBG	*International Biometric Group.* 64

IDE	*Integrated Development Environment*. 55, 56
IQS	*Image Quality Specification*. 17, 18
KNN	*k-Nearest Neighbors*. 59, 74
L3TK	*Level 3 Fingerprint Image Toolkit*. 64
LivDet	*Liveness Detection Competition*. 46, 48–51, 61, 73, 85
MLP	*Multilayer Perceptron*. 59, 74
NFIQ	NIST *Fingerprint Image Quality Measure*. 41, 58, 81, 82, 84
NIST	*National Institute of Standards and Technology*. 58, 81, 82, 84
ODA	*Overall Detection Accuracy*. 64, 67, 68, 70, 71
OPF	*Optimum-Path Forest*. 59, 74
PD	*Pore Diference*. 41
PIV	*Personal Identity Verification*. 17, 18
ROC	*Receiver Operating Characteristics*. 23
ROI	*Region of Interest*. 41
SDK	*Software Development Kit*. 56, 64
SVM	*Support Vector Machine*. 59, 73, 74
TCP/IP	*Transmission Control Protocol/Internet Protocol*. 26
TDR	*True Detection Rate*. 63, 67, 68, 70, 71
TSE	*Tribunal Superior Eleitoral*. 2

UNESP-FSDB UNESP *Fingerprint Spoof Database*. v, vi, 51, 52, 54, 56, 61–65, 67, 69, 71–76, 78–81, 83–86, 90

WEKA *Waikato Environment for Knowledge Analysis*. 56, 59

Capítulo 1

Introdução

Atualmente existe uma preocupação muito grande em identificar pessoas. Diariamente milhões de pessoas são questionadas acerca de sua identidade em diversas situações que vão desde o acesso ao local de trabalho ou estudo, sistemas de informação, caixas eletrônicos e controle de fronteiras, até a prevenção de ataques terroristas. Diante disso, tem surgido uma grande demanda por sistemas de identificação precisa, rápida e segura de pessoas. Métodos tradicionais de identificação são baseados em posses, como chaves, documentos, *tokens*, cartões ou carteira de motorista, ou baseados em conhecimento, como senhas, dados pessoais ou informações particulares. Entretanto, esses métodos não são confiáveis para estabelecer a identidade de uma pessoa, pois, posses podem ser perdidas, roubadas ou usadas por outras pessoas e o conhecimento pode ser esquecido ou adivinhado por outrem (Jain et al., 2008).

Como os métodos tradicionais possuem vulnerabilidades, surgiu a biometria, que refere-se ao uso de características físicas (face, íris, impressões digitais) ou comportamentais (voz, assinatura, modo de andar), chamados de identificadores biométricos, para reconhecimento automático de pessoas (Jain & Maltoni, 2009).

Diversas características biométricas estão sendo objeto de pesquisa para a identificação biométrica de pessoas. Apesar de ser uma das características mais antigas utilizadas para identificação humana, principalmente em aplicações forenses, as impressões digitais continuam sendo amplamente utilizadas para tais aplicações e, mais recentemente, passaram a ser também amplamente utilizadas em aplicações comerciais e governamentais. Dentre as principais aplicações que utilizam impressões digitais podemos citar a identificação de eleitores brasileiros por meio de urnas eletrônicas biométricas, o controle de fronteiras e imigração por meio dos passaportes, o controle de acesso ao local de trabalho por meio dos relógios de ponto biométricos,

o acesso aos serviços bancários por meio de caixas bancários eletrônicos biométricos, entre outros.

Apesar do avanço nas pesquisas envolvendo o reconhecimento automático de impressões digitais, poucos trabalhos investigam os possíveis ataques que sistemas de reconhecimento biométricos baseados nesta característica podem sofrer. Com o aumento da utilização destes sistemas, as tentativas de ataque também aumentam. Desta forma, o desenvolvimento de técnicas para prevenir fraudes são cada vez mais cruciais.

1.1 Objetivos

Esta dissertação de mestrado tem os seguintes objetivos:

- Fazer uma revisão da literatura sobre técnicas para detecção de impressões digitais falsas, apresentando as principais abordagens, visando compreender suas propriedades, princípios e desempenho;

- Propor um método robusto para detecção de impressões digitais falsas utilizando estatísticas de primeira ordem dos tons de cinza da impressão digital, medida de qualidade da impressão digital, juntamente com características de terceiro nível que podem ser utilizadas para reconhecimento robusto de impressões digitais, como os poros de transpiração;

- Criação de uma nova base de dados com impressões digitais provenientes de dedos verdadeiros e impressões digitais provenientes de dedos sintéticos, contendo imagens com 500 e 1000 dpi, sendo estas últimas consideradas como de alta resolução.

- Avaliar o desempenho do método proposto considerando alguns fatores que podem influenciar no desempenho, tais como: (i) resolução da imagem da impressão digital 500dpi e 1000dpi; (ii) utilização de características de terceiro nível (poros); (iii) pressão do dedo sobre a superfície do sensor; (iv) tempo de aquisição da imagem da impressão digital; (v) umidade presente no dedo no momento da captura da impressão digital.

1.2 Motivação

Atualmente, existem muitas pesquisas sendo conduzidas com foco no aperfeiçoamento dos sistemas automáticos de reconhecimento, extração de características, identificação e indexação de impressões digitais. Tal aperfeiçoamento, aliado com a redução dos custos de implantação de sistemas biométricos, principalmente os baseados em impressões digitais, levam ao aumento expressivo da quantidade e tipos de aplicações em que a biometria passou a ser utilizada. Um exemplo importante de identificação biométrica no Brasil refere-se ao Tribunal Superior Eleitoral brasileiro, que aprovou e está implantando paulatinamente a identificação biométrica dos eleitores brasileiros por meio do reconhecimento das impressões digitais nas urnas eletrônicas. Nas eleições de 2014, mais de 23 milhões de eleitores brasileiros foram identificados pelas impressões digitais, a meta do *Tribunal Superior Eleitoral* (TSE) é poder identificar todos os eleitores brasileiros desta forma (Tribunal Superior Eleitoral, 2014).

No setor privado observa-se também um aumento da utilização de biometria para registro de ponto dos funcionários, acesso a locais restritos, para assegurar o acesso aos serviços disponibilizados pelas operadoras de planos de saúde, etc.

Por outro lado, existem poucas pesquisas sendo realizadas para a detecção e prevenção de fraudes e ataques em sistemas biométricos, fato esse que motivou no Brasil a proposição do Projeto de Lei 3558/2012, que dispõe sobre a utilização de sistemas biométricos, a proteção de dados pessoais e dá outras providências (Brasil, 2012). Este Projeto de Lei visa regulamentar a utilização de sistemas biométricos de forma segura e confiável, protegendo as pessoas que o utilizam. Neste projeto de lei estão previstas infrações administrativas para ações ou omissões que violem as regras jurídicas de uso e proteção ou vulnerem a privacidade dos dados biométricos, que serão punidas com as seguintes sanções: advertência, multa simples, suspensão de venda e fabricação do produto e suspensão das atividades.

No projeto de lei também está previsto o crime de modificação de dados em sistema de informações, onde, inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos obtidos mediante a utilização de biometria com o fim de obter vantagem indevida para si ou para outrem ou para causar dano é tipificado como um crime com pena de reclusão, de 1(um) a 4(quatro) anos, e multa(Brasil, 2012).

O problema de detecção de impressões digitais falsas é, portanto, bastante atual e relevante e esta dissertação de mestrado visa contribuir para o avanço do estado da arte na área de biometria e aumentar a segurança de sistemas biométricos.

1.3 Estrutura da Dissertação

Além deste capítulo introdutório, que também apresentou os objetivos e motivações para este trabalho, esta monografia contém mais cinco capítulos.

No Capítulo 2 são introduzidos os principais termos e conceitos de Biometria abordados neste trabalho, trazendo também os modos de operação dos sistemas biométricos, as medidas de desempenho comumente utilizadas para avaliação destes sistemas, os principais ataques que os sistemas biométricos podem sofrer e os ataques específicos para sistemas baseados em impressões digitais.

No Capítulo 3 são abordadas as técnicas descritas na literatura para detecção de impressões digitais falsas, a saber: técnicas baseadas na análise do padrão de transpiração, técnicas baseadas na análise das características de terceiro nível e técnicas baseadas em medidas de estatísticas de primeira ordem dos tons de cinza das imagens das impressões digitais.

No Capítulo 4 são descritos a metodologia empregada nesta dissertação, os métodos utilizados, com detalhes acerca dos parâmetros adotados, e o material utilizado para avaliação dos métodos.

No Capítulo 5 são apresentados os resultados dos experimentos realizados e é conduzida uma discussão acerca do método proposto para a detecção de impressões digitais falsas, considerando alguns fatores como: resolução do sensor, utilização de características de terceiro nível, influência da pressão utilizada no momento da captura, tempo de aquisição da impressão digital e umidade presente no dedo no momento da captura.

Por fim, no Capítulo 6 são apresentadas as conclusões desta dissertação, são enumeradas as contribuições deste estudo e apontados os trabalhos futuros que poderão ser desenvolvidos a partir do que foi realizado nesta dissertação.

Capítulo 2

Biometria e Impressões Digitais

Neste capítulo são apresentados os principais conceitos sobre biometria, reconhecimento de impressões digitais e tipos de ataques a sistemas biométricos.

2.1 Introdução à Biometria

Biometria é um campo que vem sendo explorado largamente tanto pela indústria quanto pela academia por meio do desenvolvimento de pesquisas para introduzir novos métodos de reconhecimento, bem como para melhorar os existentes. Dentre as áreas que utilizam biometria podemos destacar: identificação forense e civil, controle de ponto de funcionários, controle de acesso físico e lógico em áreas de segurança, autenticação de transações bancárias, dentre outras.

Muitas características podem ser utilizadas nos sistemas biométricos, cada uma delas tem os seus prós e contras, ou seja, nenhuma característica biométrica é perfeita. Portanto, a escolha de uma característica biométrica depende muito do contexto de utilização e de quais fatores são mais importantes para o sistema. Sete propriedades podem ser analisadas para determinar se uma característica física ou comportamental pode ser utilizada como identificador biométrico (Jain et al., 2008):

- *Universalidade:* todas as pessoas da população a ser identificada devem possuir a característica;
- *Unicidade:* a característica ser suficientemente única para cada pessoa de tal modo que possa permitir diferenciá-la em uma população;
- *Permanência:* a característica não deve sofrer alterações significativas com o passar do tempo;

- *Coletabilidade:* a característica deve ser fácil de ser coletada e medida quantitativamente;
- *Desempenho:* a característica deve possibilitar um reconhecimento preciso, rápido e utilizando pouca memória;
- *Aceitabilidade:* a característica deve ser aceita pela população que será identificada;
- *Circunvenção:* a característica deve ser difícil de ser fraudada.

Na Tabela 2.1 é apresentado um comparativo entre as principais características biométricas.

Tabela 2.1: Comparação das características biométricas mais utilizadas (Jain & Maltoni, 2009).

Característica	**Universalidade**	**Unicidade**	**Permanência**	**Coletabilidade**	**Desempenho**	**Aceitabilidade**	**Circunvenção**
Face	Alta	Baixa	Média	Alta	Baixa	Alta	Baixa
Impressão Digital	Média	Alta	Alta	Média	Alta	Média	Média
Geometria das mãos	Média	Média	Média	Alta	Média	Média	Média
Veias da mão/dedo	Média	Média	Média	Média	Média	Média	Alta
Íris	Alta	Alta	Alta	Média	Alta	Baixa	Alta
Assinatura	Baixa	Baixa	Baixa	Alta	Baixa	Alta	Baixa
Voz	Média	Baixa	Baixa	Média	Baixa	Alta	Baixa

Apesar de ser uma característica que não possui o melhor desempenho em todas as propriedades, a impressão digital é muito utilizada para identificação de pessoas, pois possui uma boa unicidade (até mesmo gêmeos idênticos possuem impressões digitais diferentes) e apresenta uma boa permanência, desse modo mesmo com mudanças temporárias (causadas por ferimentos) ela se regenera, voltando à forma inicial e não impactando negativamente no reconhecimento (Jain & Maltoni, 2009).

O reconhecimento biométrico utilizando impressões digitais é uma das tecnologias biométricas mais maduras e mais utilizadas, tanto para aplicações forenses quanto para aplicações comerciais e governamentais.

A eficiência de um sistema de autenticação, seja ele baseado em biometria ou não, é baseada na relevância da aplicação em particular e no quão robusta a aplicação é para os mais variados tipos de ataques (Jain et al., 2008).

Em sistemas baseados em senhas e *tokens* os seguintes ataques podem acontecer:

- Ataque ao cliente (adivinhar a senha, roubar o *token*);
- Ataque ao computador (acessar um arquivo texto contendo as senhas);
- Escutas (*software* que captura informações da rede);
- Cavalo de Troia (instalação de tela falsa de *login* para capturar senhas);
- Repúdio (alegando que a senha foi roubada ou o *token* extraviado);
- Ataques de negação de serviço (desabilitar o sistema informando uma senha incorreta várias vezes).

Embora muitos destes ataques possam ser evitados utilizando-se mecanismos apropriados de defesa, não é possível eliminar todos os problemas associados à utilização de senhas e *tokens*.

A biometria, por sua vez, oferece algumas vantagens como a identificação negativa e o não repúdio. A identificação negativa rejeita a alegação de não identidade, caso haja casamento entre a amostra e os templates armazenados no banco de dados, a finalidade da identificação negativa é prevenir uma pessoa de usar múltiplas identidades. O não repúdio é um meio de garantir que um indivíduo que acessou o sistema não possa depois negar que o tenha feito (Jain et al., 2004).

Sistemas biométricos podem utilizar uma variedade de características físicas ou comportamentais, conforme ilustra a Figura 2.1, incluindo impressões digitais, face, geometria da mão, íris, retina, assinatura, forma de andar, impressão da palma da mão, padrão da voz, orelha, padrão de veias da mão, odor ou até mesmo as informações do *Ácido Desoxirribonucleico* (DNA) de uma pessoa para determinar sua identidade. Apesar de sistemas biométricos possuírem limitações, eles têm uma vantagem sobre os métodos tradicionais de identificação, pois as características biométricas são mais difíceis de serem roubadas ou compartilhadas. Além de aumentar a segurança, sistemas biométricos também facilitam a vida dos usuários que não necessitam criar e memorizar inúmeras senhas.

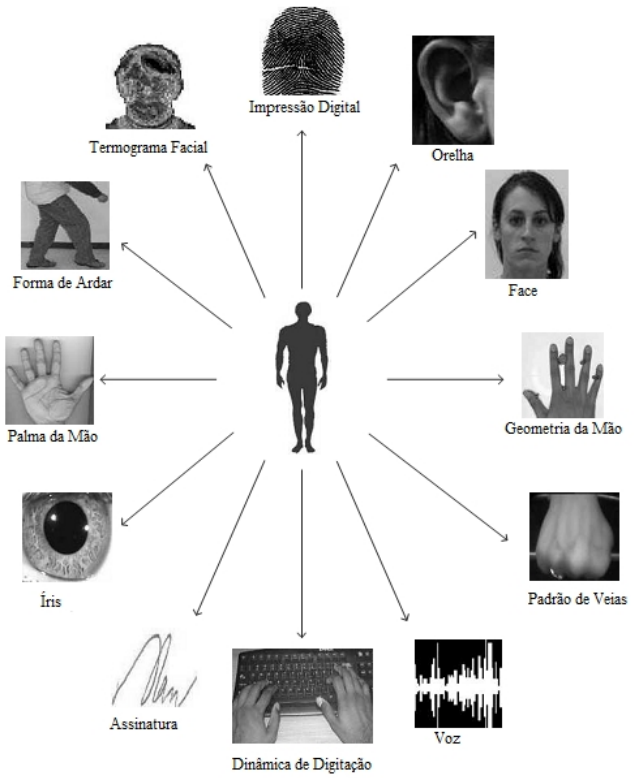


Figura 2.1: Exemplos de características biométricas que podem ser utilizadas para identificar um indivíduo. Adaptado de (Jain et al., 2008).

2.2 Impressões Digitais Como Característica Biométrica

Entre os sistemas biométricos, os baseados em impressões digitais são provavelmente os mais conhecidos e mais difundidos devido as suas propriedades: universalidade, permanência, coletabilidade, desempenho, aceitabilidade, circunvenção e unicidade (Ghiani et al., 2013). A impressão digital é formada pelo padrão de cristas e vales que são encontrados nas pontas dos dedos conforme ilustra a Figura 2.2. Este padrão é formado durante os sete primeiros meses de gestação e permanece inalterado no decorrer da vida do indivíduo (Jain & Maltoni, 2009).

As impressões digitais são utilizadas para reconhecimento humano desde o início do século XX e a acurácia do reconhecimento é muito alta (Jain et al., 2004). Atualmente, devido ao baixo custo dos sensores que capturam impressões digitais a utilização de sistemas biométricos baseados em impressões digitais é cada vez maior.

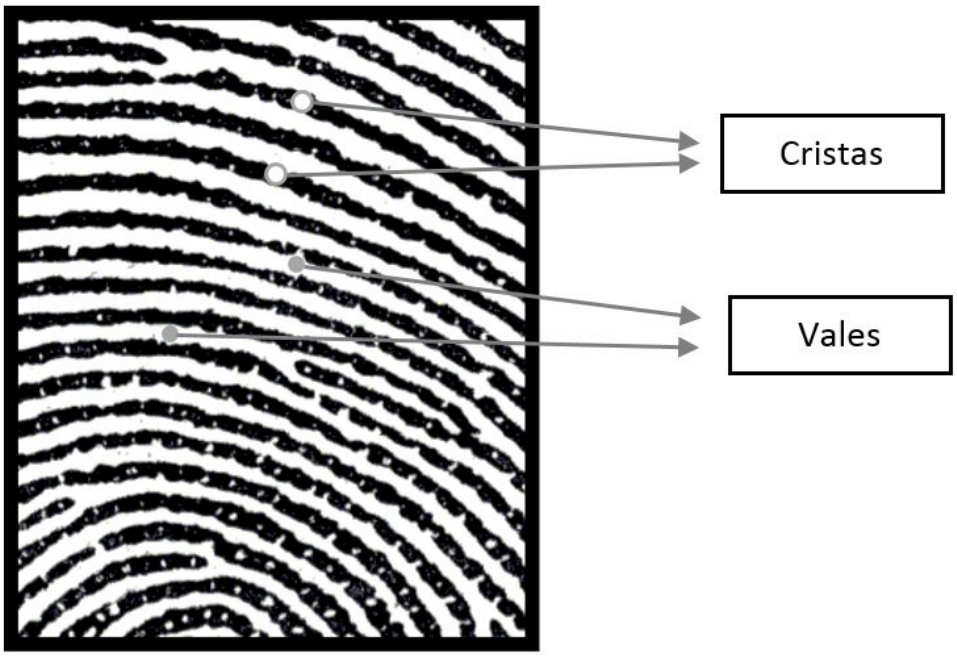


Figura 2.2: Cristas e vales em uma impressão digital.

As características das impressões digitais utilizadas para efetuar a identificação de pessoas são classificadas em primeiro, segundo e terceiro níveis.

O primeiro nível de características consiste no padrão dos macro detalhes da impressão digital, formado pelo fluxo das cristas e vales. Esse padrão não é suficientemente discriminativo para identificar os indivíduos, mas pode ser utilizado para classificar as impressões digitais em seis categorias (arco, arco tenda, laço esquerdo, laço direito, laço duplo e verticilo) e, desse modo, permitir a indexação do banco de dados e tornar as buscas mais rápidas.

O segundo nível de características consiste nos detalhes locais também chamados de minúcias, dentre os quais destacam-se os pontos de terminações e bifurcações das cristas.

O terceiro e último nível consiste em todos os atributos dimensionáveis das cristas, tais como: largura, contorno, forma, poros sudoríparos, dobras, cicatrizes e outros detalhes permanentes. A Figura 2.3 mostra os elementos que compõem os três níveis de características em uma impressão digital (Jain & Maltoni, 2009).

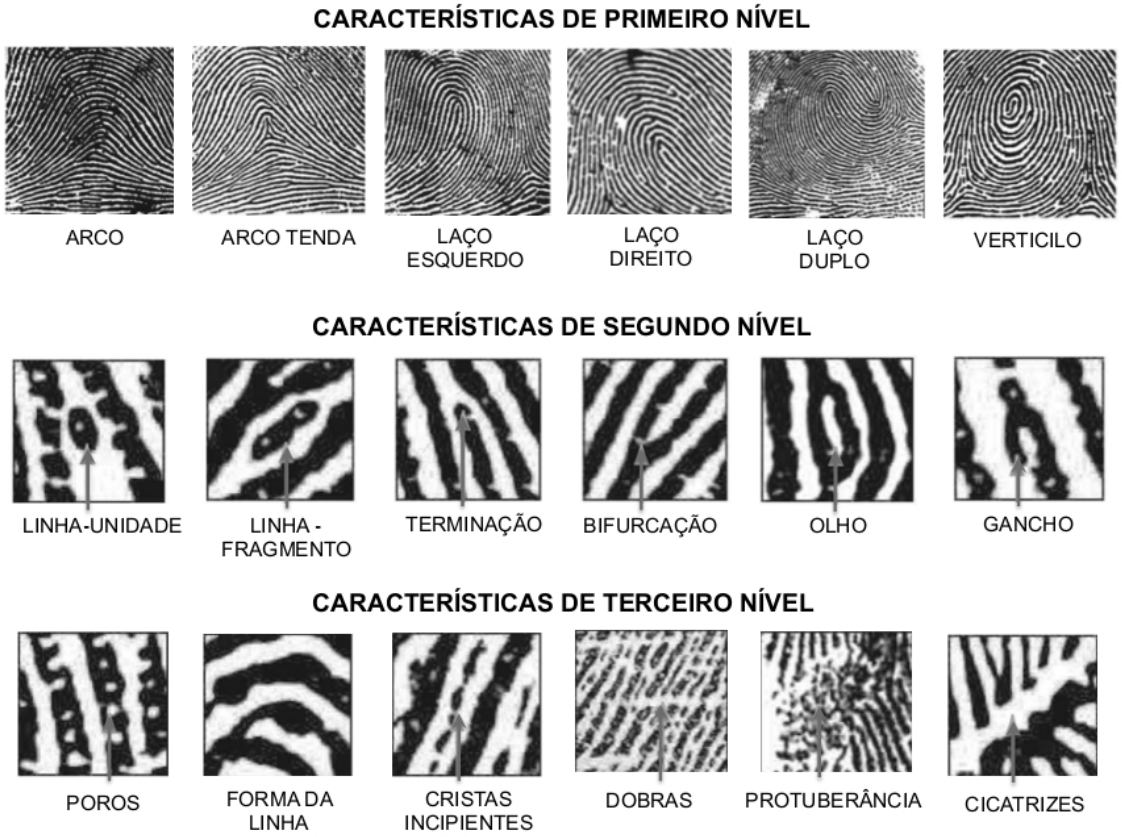


Figura 2.3: Elementos que compõem os três níveis de características das impressões digitais. Adaptado de (Jain et al., 2007).

2.3 Tipos de Sensores de Impressões Digitais

Para a aquisição das imagens das impressões digitais podem ser utilizados diversos tipos de sensores (ópticos, capacitivos, ultrassônicos, etc). Uma estrutura padrão de funcionamento de um sensor de impressões digitais é mostrada na Figura 2.4. Como pode ser observado, o sensor efetua a leitura do padrão de cristas da superfície do dedo e converte o sinal analógico recebido em um sinal digital por meio do módulo conversor analógico/digital. Um módulo de interface é responsável pela comunicação com o dispositivo externo, como por exemplo um computador.

O desenvolvimento de sistemas biométricos seguros baseados em impressões digitais requer a implementação de mecanismos de proteção nos sensores e de criptografia no processo de comunicação do sensor com o dispositivo externo e também entre os módulos do sistema biométrico. Na Seção 2.5 são apresentadas as vulnerabilidades mais comuns dos sistemas biométricos, e as técnicas de contramedida propostas para

aumentar a segurança em sistemas contra os mais variados tipos de ataques e, em particular, para detectar impressões digitais falsas que podem ser apresentadas aos sensores.

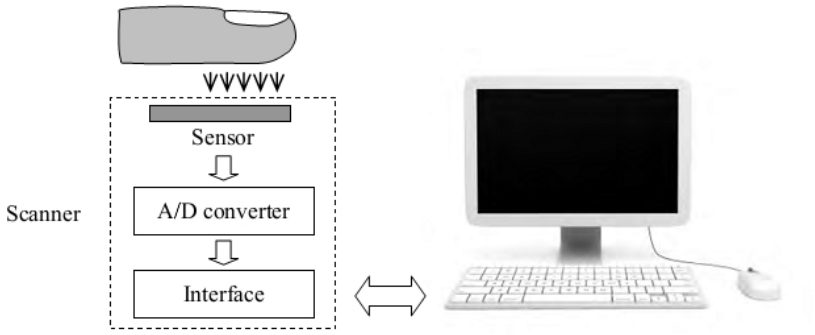


Figura 2.4: Diagrama de funcionamento de um sensor de impressões digitais (Jain & Maltoni, 2009).

Segundo Jain & Maltoni (2009) os sensores de impressões digitais podem ser classificados nas seguintes categorias:

- **Multi-Dedos:** mais de um dedo pode ser capturado simultaneamente conforme ilustra a Figura 2.5 (a). Nestes sensores, geralmente os quatro dedos da mão, exceto o polegar, podem ser capturados ao mesmo tempo, assim três aquisições são suficientes para capturar todas as dez impressões digitais em sequência: quatro dedos (mão direita), quatro dedos (mão esquerda), e os dois polegares juntos. Após este processo de captura é realizada a segmentação para separar a imagem que contém quatro impressões digitais em quatro imagens, cada uma contendo a impressão de um dos dedos. Este processo de segmentação é conhecido como *slap segmentation*, e esta etapa geralmente é realizada por *software* como mostrado na Figura 2.6.

- **Único-Dedo:** apenas um dedo é capturado por vez conforme ilustra a Figura 2.5 (b). Este tipo de sensor é o mais utilizado em aplicações comerciais e pessoais devido ao seu pequeno tamanho, baixo custo e simplicidade de uso. Um *design* compacto e um baixo custo são cruciais para permitir a utilização de sensores de impressões digitais embutidos em dispositivos móveis como *notebooks* e *smartphones*. Por isso, os sensores de varredura ou deslizamento são os mais empregados nesses tipos de equipamentos. Os sensores de deslizamento adquirem uma sequência de imagens parciais da impressão do dedo, que depois

são combinadas por meio de técnicas de mosaicagem para obter a imagem inteira da impressão digital.

Figura 2.5: Sensores de impressões digitais. a) Captura simultânea de 4 dedos um sensor multi-dedos. b) Captura com um sensor de apenas um dedo. Adaptado de (Jain & Maltoni, 2009).

Figura 2.6: Um exemplo de imagem com 500dpi capturada com um scanner multi-dedos Papillon DS-30, os quatro retângulos mostram a posição das quatro impressões digitais localizadas por um algoritmo de segmentação automática. Adaptado de (Jain & Maltoni, 2009).

Sensores ópticos (ou *Frustrated Total Internal Reflection* (FTIR)), são os mais antigos e mais utilizados atualmente para captura de impressões digitais. Conforme o dedo toca o lado superior de um prisma, que pode ser de vidro ou plástico, as cristas entram em contato com a superfície do prisma, porém, os vales se mantém a uma certa distância, conforme ilustra a Figura 2.7. O outro lado do prisma é iluminado por meio de uma luz difusa, geralmente por um conjunto de LEDs. A luz que entra no prisma é refletida pelos vales e se espalha aleatoriamente nas cristas que a absorvem. A ausência de reflexão permite que as cristas (partes pretas da imagem)

sejam diferenciadas dos vales (partes brancas da imagem). Os raios de luz que saem do lado oposto do prisma são focados, por meio de uma lente, a um sensor de imagem CCD ou CMOS. Como os sensores ópticos são sensíveis à superfície tridimensional do dedo, eles não podem ser enganados com a apresentação de uma fotografia de uma impressão digital (Jain & Maltoni, 2009).

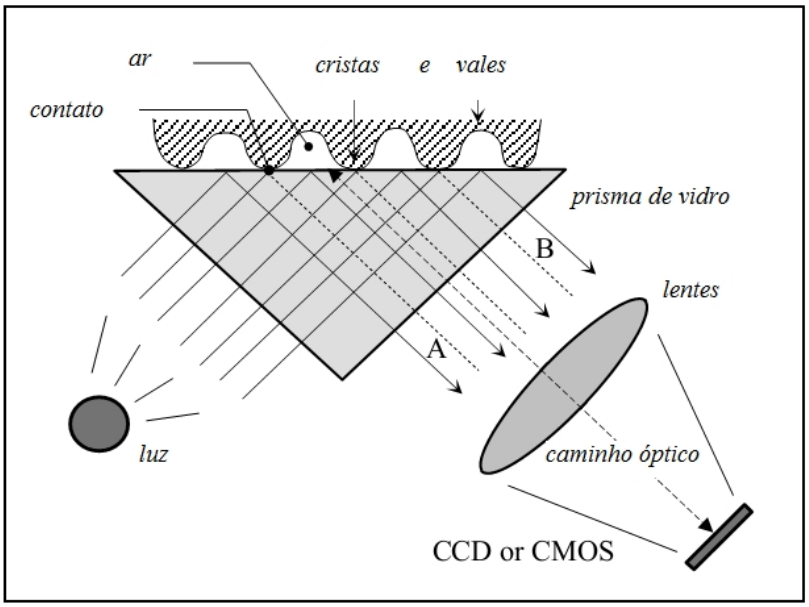


Figura 2.7: Sensor óptico (FTIR) em operação. Adaptado de (Jain & Maltoni, 2009).

Sensores capacitivos, também conhecidos como sensores de estado sólido ou sensores de silício, foram inicialmente projetados na década de 80, porém, apenas na década de 90 tornaram-se comerciais. O desenvolvimento desse tipo de sensor se deu para superar os problemas de custo e tamanho dos sensores, que na época pareciam ser um impedimento para utilização generalizada de sistemas biométricos baseados em impressões digitais. Todos os sensores baseados em silício consistem de uma matriz de pixels, sendo cada pixel um sensor minúsculo. Como o usuário toca diretamente na superfície de silício, não são necessários componentes ópticos ou os sensores de imagem CCD ou CMOS (Jain & Maltoni, 2009). Dentre as tecnologias utilizadas em sensores de estado sólido, quatro principais têm sido propostas para converter o padrão de impressões digitais em sinais elétricos: capacitiva, térmica, campo elétrico, e piezoelétricos. Embora existam outras tecnologias para fabricação de sensores de estado sólido, os sensores capacitivos são os mais utilizados com tecnologia baseada em silício e como são sensíveis à superfície tridimensional do dedo, eles não podem ser enganados com a simples apresentação de uma fotografia de uma

impressão digital. Um sensor capacitivo com uma matriz bidimensional de micro capacitores é ilustrado na Figura 2.8.

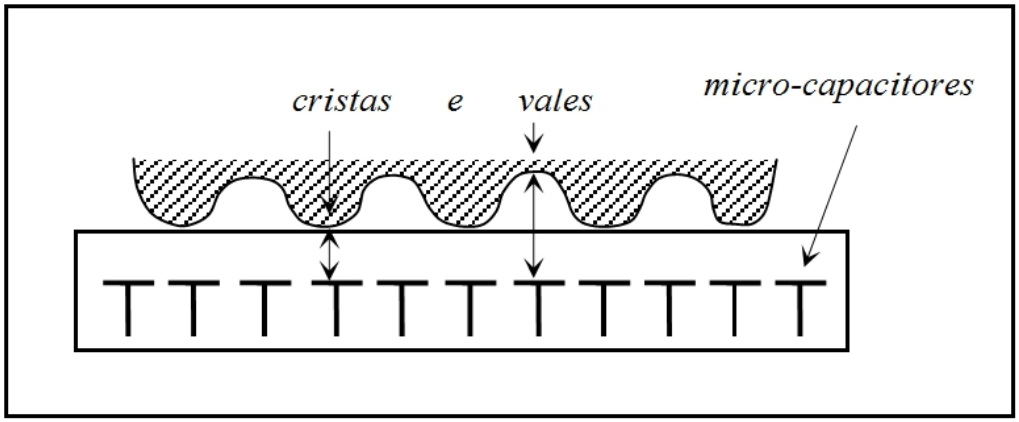


Figura 2.8: Sensor capacitivo. Adaptado de (Jain & Maltoni, 2009).

Sensores ultrassônicos podem ser comparados a um tipo de sonar, pois são baseados no envio de sinais acústicos para a ponta do dedo e a captura do sinal do eco. O sinal do eco é utilizado para calcular a distância ou profundidade da imagem da impressão digital e, consequentemente, o padrão de cristas e vales, conforme mostra a Figura 2.9. Um sensor ultrassônico possui dois componentes principais: um transmissor que gera pequenos pulsos acústicos, e um receptor que detecta a resposta obtida quando um pulso rebate na superfície da impressão digital. Este método captura informações subcutâneas e é capaz de funcionar mesmo através de luvas finas. É, portanto, resistente a pequenas sujeiras e óleos que podem se acumular nos dedos.

Sensores ultrassônicos não podem ser fraudados com a simples apresentação de uma fotografia da impressão digital, pois utilizam a estrutura tridimensional do dedo para detectar o padrão das cristas e vales e são capazes de gerar imagens de boa qualidade. Entretanto, os dispositivos que utilizam esta tecnologia atualmente são muito grandes, caros e compostos de peças mecânicas. Além disso, ele leva alguns segundos para capturar a imagem. Portanto, esta tecnologia ainda não está madura o suficiente para ser utilizada em larga escala (Jain & Maltoni, 2009).

Existem diversos tipos de sensores baseados em várias tecnologias que estão disponíveis no mercado e as características necessárias em um sensor estão diretamente ligadas a sua aplicação. Por isso, o *Federal Bureau of Investigation* (FBI) define alguns parâmetros principais para aquisição de imagens de impressões digitais:

- **Resolução:** indica o número de pontos ou pixels por polegada (*Dots per Inch* (dpi)). Uma resolução de 500dpi é a resolução mínima para um *scanner* ser

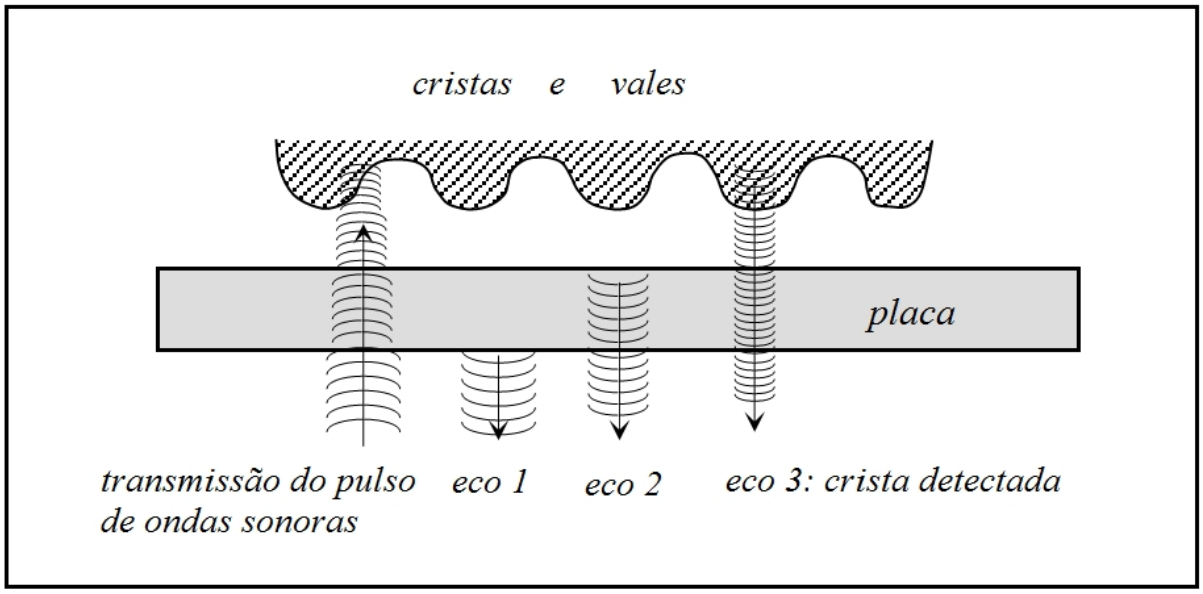


Figura 2.9: Sensor ultrassônico. Adaptado de (Jain & Maltoni, 2009).

compatível com as normas de qualidade do FBI e é encontrada na maioria dos *scanners* comerciais. A Figura 2.10 mostra a mesma impressão digital capturada em diferentes resoluções. Pode-se observar que ao diminuir a resolução fica mais difícil de identificar o padrão de cristas e vales. *Scanners* de 1000dpi surgiram para substituir os *scanners* de 500dpi inicialmente em aplicações forenses, onde os peritos analisam pequenos detalhes das impressões digitais, as chamadas características de terceiro nível, como poros sudoríparos, pontos, cristas incipientes, etc. A Figura 2.11 mostra a mesma impressão digital capturada em 1000 e 500 dpi.

- **Área:** indica o tamanho da área retangular que pode ser capturada por um sensor de impressão digital. A área de aquisição para sensores multi-dedos é geralmente de 2 X 3 polegadas quadradas que permite escanear até quatro dedos simultaneamente, já para os sensores de único dedo, uma área de 1 X 1 polegada quadrada ou maior permite capturar impressões digitais completas.

- **Número de Pixels:** o número de pixels em uma imagem de impressão digital pode ser obtido a partir da resolução e área do sensor: um *scanner* que trabalha com R dpi com uma área de altura (a) X largura (l) tem (R * a) * (R * l) pixels. Se a área estiver em mm^2, temos que incluir uma conversão de mm para polegadas, assim, o número de pixel = (R * (a / 25.4)) X (R * (l / 25.4)),

por exemplo, um *scanner* que trabalha com 500 dpi com uma área de 20.32 X 15.24 mm^2 gera uma imagem de (500 *(20.32/25.4)) X (500 * (15.24/25.4)) = 400 X 300 pixels.

- **Quantização e Faixa de Níveis de Cinza:** a quantização de níveis de cinza indica o número máximo de tons de cinza na imagem de saída e está relacionado com o número de bits utilizado para codificar o valor de cada pixel, como, por exemplo, 8 bits por pixel, produzindo 256 tons de cinza. Já a faixa de tons de cinza é o número real de tons de cinza utilizado em uma impressão digital, desconsiderando o máximo permitido pela quantização. Informação de cor não é considerada útil para o reconhecimento de impressões digitais, porém, alguns estudos têm mostrado que a análise da cor pode ser explorada para detectar dedos falsos.

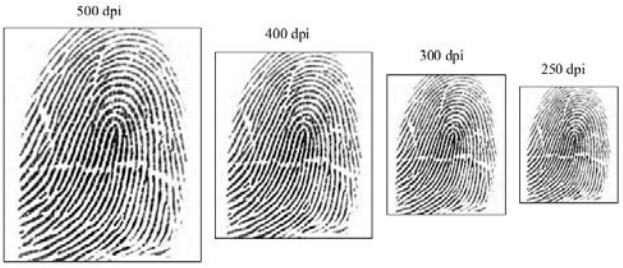


Figura 2.10: Impressão digital da esquerda capturada com 500dpi e outras amostras capturadas com menor resolução 400, 300 e 250 dpi respectivamente. Adaptado de (Jain & Maltoni, 2009).

Segundo Jain & Maltoni (2009), em muitas aplicações biométricas, dois requisitos são fundamentais: primeiro, a qualidade da imagem deve ser suficientemente alta para garantir o reconhecimento da impressão digital e, segundo, o sistema deve ser capaz de usar dispositivos de diferentes fabricantes e a acurácia do sistema não deve diminuir se o dispositivo utilizado no cadastramento for diferente do utilizado no reconhecimento.

Assim, o FBI estabeleceu uma especificação de qualidade de imagem (*Integrated Automated Fingerprint Identification System Image Quality Specification* (IAFIS IQS)), a fim de definir uma medida quantitativa de qualidade requerida para sensores *Integrated Automated Fingerprint Identification System* (IAFIS) de impressões digitais. Esta medida de qualidade tipicamente é utilizada para sensores que capturam mais de uma impressão digital simultaneamente. Por outro lado, a norma ISO/IEC 19794-4

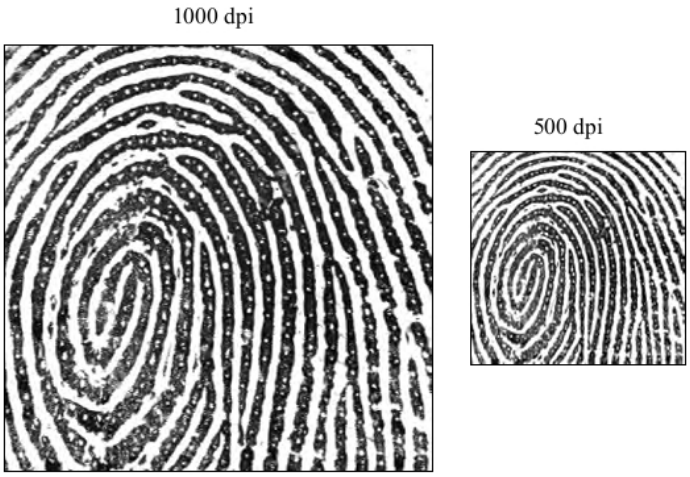


Figura 2.11: Impressão digital capturada em 1000 e 500 dpi. Adaptado de (Jain & Maltoni, 2009).

de 2005 descreve a maneira na qual a imagem de impressão digital deve ser capturada para maximizar a interoperabilidade entre os diversos sensores (Jain & Maltoni, 2009).

Para apoiar o programa de verificação de identidade pessoal (*Personal Identity Verification* (PIV)), cujo objetivo é melhorar a identificação e autenticação para acesso às instalações federais americanas e sistemas de informação, o FBI criou o *Image Quality Specification* (IQS) PIV que define os requisitos de qualidade para sensores de impressões digitais que capturam imagem de apenas um dedo por vez, adequados para utilização no programa PIV, requisitos estes semelhantes ao *Integrated Automated Fingerprint Identification System Image Quality Specification* (IAFIS IQS), porém, menos rigorosos.

As Tabelas 2.2 e 2.3 listam alguns sensores de captura de múltiplos dedos e captura de único dedo, o custo de *scanners* multi-dedo é de aproximadamente US$5.000, já o custo de *scanners* de único dedo estão na faixa de US$50 e US$500, variando de acordo com a área de aquisição e qualidade da imagem capturada.

Tabela 2.2: Alguns exemplos de sensores comerciais de impressão digital de multi-dedo, baseados em tecnologia óptica FTIR. Adaptado de (Jain & Maltoni, 2009).

	Tecnologia	**Empresa**	**Modelo**	***Dots per Inch* (dpi)**	**Área**	**Compatível IAFIS IQS**
Óptico	FTIR	Crossmatch www.crossmatch.net	L SCAN 1000	1000	3.0"X3.2"	Sim
	FTIR	L-1 Identity www.l1id.com	TouchPrint 4100	500	3.0"X3.2"	Sim
	FTIR	Papillon www.papillon.ru	DS-30	500	3.07"X3.38"	Sim

Tabela 2.3: Sensores comerciais de único dedo, agrupados por tecnologia. Adaptado de (Jain & Maltoni, 2009).

	Tecnologia	Empresa	Modelo	DPI	Área	Compatível PIV IQS
Óptico	FTIR	Biometrika www.biometrika.it	HiScan	500	1"X1"	Sim
	FTIR	Crossmatch www.crossmatch.net	Verifier 300 LC 2.0	500	1.2"X1.2"	Não
	FTIR	Digital Persona www.digitalpersona.com	UareU4000	512	0.71"X0.57"	Não
	FTIR	L-1 Identity www.identix.com	DFR 2100	500	1.05"X1.05"	Sim
	FTIR	Sagem www.morpho.com	MSO350	500	0.86"X0.86"	Sim
	FTIR	Secugen www.secugen.com	Hamster IV	500	0.66"X0.51"	Sim
Estado Sólido	Capacitivo	Upek www.upek.com	TouchChip TCS1	508	0.71"X0.50"	Sim
	Térmico (*Sweep*)	Atmel www.atmel.com	FingerChip AT77C101B	500	0.02"X0.55"	Não
	Campo Elétrico	Authentec www.authentec.com	AES4000	250	0.38"X0.38"	Não
	Piezoelétrico	BMF www.bm-f.com	BLP-100	406	0.92"X0.63"	Não

A Figura 2.6 mostra uma imagem capturada com um *scanner* para múltiplos dedos e o resultado de uma segmentação automática. A Figura 2.12 mostra impressões digitais do mesmo dedo capturadas por alguns *scanners* de único dedo listados na Tabela 2.3.

2.4 Análise de Performance em Sistemas Biométricos

Sistemas biométricos são bem diferentes de sistemas convencionais baseados em senhas, onde um perfeito reconhecimento entre duas cadeias de caracteres é necessário para definir a identidade de uma pessoa. Por outro lado, um sistema biométrico raramente encontra duas amostras de características biométricas de um indivíduo que resulte no mesmo vetor de características, isso devido a condições imperfeitas de sensoriamento, alterações na característica biométrica do usuário, mudanças nas condições ambientais e variações na interação do usuário com o sensor. Assim, raramente dois vetores de características originados da mesma característica biométrica de um usuário serão exatamente iguais, logo, um perfeito casamento entre dois vetores de características pode indicar que um ataque de repetição (ou *replay*) está sendo lançado contra o sistema biométrico (Jain et al., 2008).

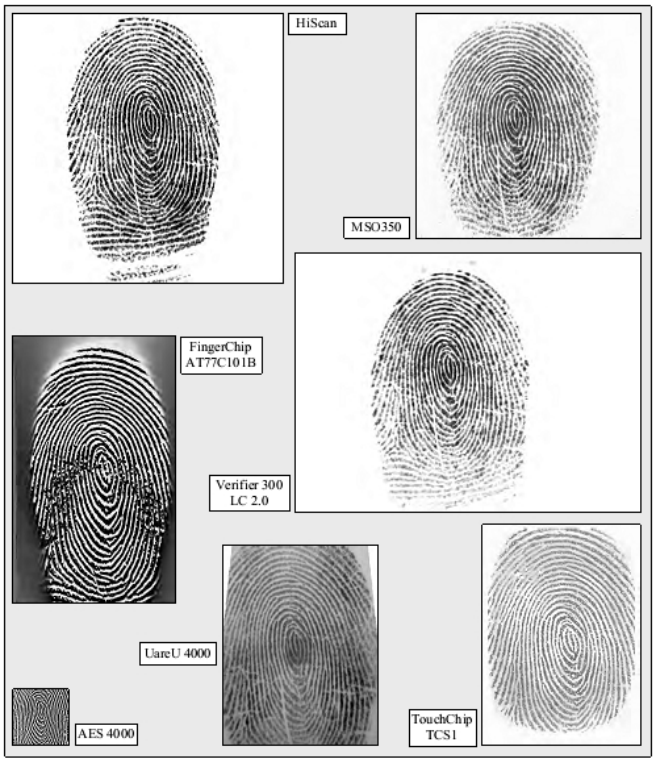


Figura 2.12: Impressões digitais capturadas do mesmo dedo com alguns *scanners* de único-dedo. Adaptado de (Jain & Maltoni, 2009).

De acordo com Jain & Maltoni (2009), um aspecto importante no desenvolvimento de um sistema biométrico é determinar como um indivíduo será reconhecido. Dependendo do contexto, um sistema biométrico pode ser chamado de sistema de verificação ou um sistema de identificação.

Um sistema de verificação autentica a identidade de uma pessoa comparando a característica capturada no sensor com sua própria característica capturada previamente na fase de cadastro e armazenada no banco de dados do sistema. Assim, tem-se uma comparação um-para-um, para confirmar se a pessoa é quem ela afirma ser. Um sistema de verificação apenas aceita ou rejeita um pedido de identidade submetido.

Por outro lado, um sistema de identificação efetua o reconhecimento de uma pessoa através da pesquisa da característica apresentada ao sensor por todo o banco de dados. Assim, tem-se comparações um-para-muitos para estabelecer se uma pessoa está presente na base de dados. Se estiver retorna o identificador de referência correspondente a sua inscrição. Em um sistema de identificação é estabelecida a

identidade de uma pessoa ou detectado que esta pessoa não possui cadastro no banco de dados, isso sem que o indivíduo declare sua identidade.

Na Figura 2.13 são retratados os principais módulos de um sistema biométrico de verificação ou identificação e o processo de cadastro, que é comum para ambos os modos de operação.

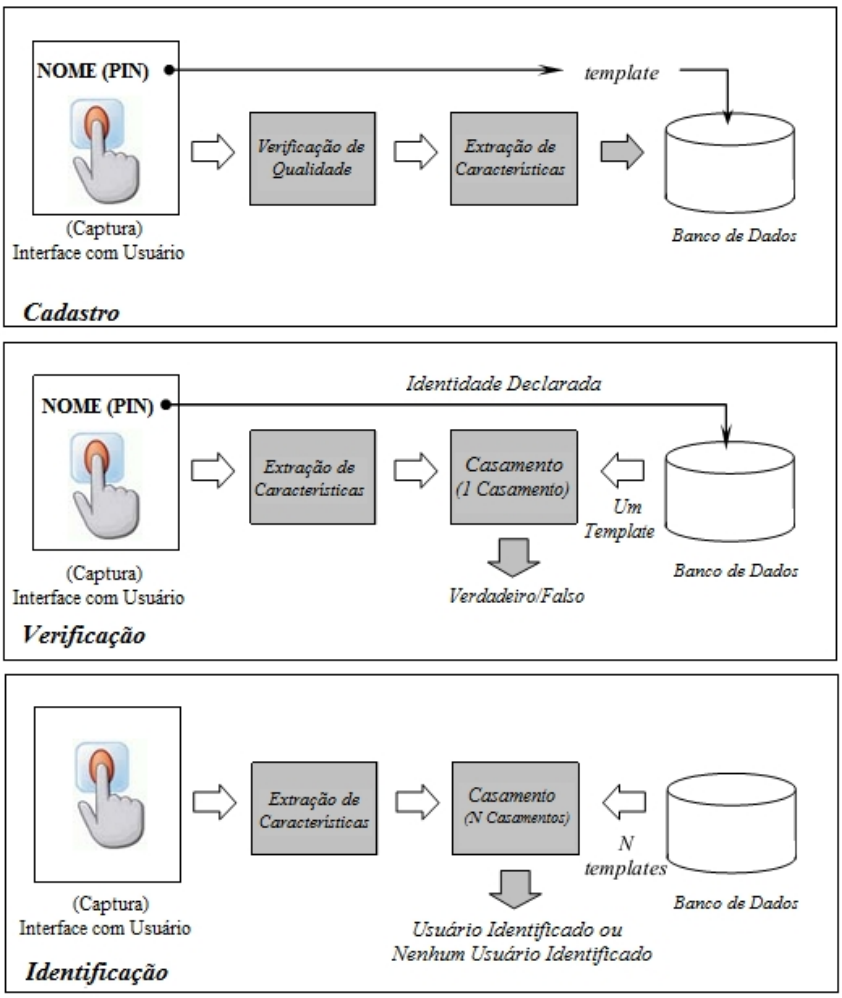


Figura 2.13: Processos de Cadastro, Verificação e Identificação biométrico. Adaptado de (Jain et al., 2004).

Os processos de cadastro, verificação e identificação para reconhecimento biométrico usam os seguintes módulos do sistema:

- **Módulo de Captura:** uma representação digital da característica biométrica tem que ser detectada e capturada. Portanto, um sensor biométrico como um leitor de impressões digitais é uma das peças centrais do módulo de captura. A

representação digital capturada da característica biométrica é com frequência chamada de amostra. Por exemplo, em sistemas biométricos baseados em impressões digitais, a imagem da impressão digital capturada pelo sensor é a amostra. O módulo de captura pode também conter outros equipamentos, como um teclado para obter outras informações.

- **Módulo de Extração de Características:** para facilitar a etapa de casamento ou comparação, a representação digital de uma característica biométrica, ou simplesmente amostra, é processada pelo extrator de características que gera uma representação compacta da amostra, denominada vetor de características.

- **Módulo de Criação do Template:** Este módulo organiza um ou muitos vetores de características extraídos dentro de um modelo (template) para o cadastramento no banco de dados.

- **Pré-Seleção e Casamento:** Pré-seleção ou filtro é realizada antes da etapa de casamento no processo de identificação quando o número de templates cadastrados é grande. Esta abordagem é utilizada para reduzir o número de templates que serão comparados para um número relativamente pequeno. A etapa de casamento ou comparação calcula a medida de similaridade entre as amostras cadastradas na base de dados (template) e a amostra de consulta retornando uma pontuação. Esta pontuação é comparada com um limiar (*threshold*) para tomar a decisão final. Se a pontuação for maior que o limiar a pessoa é reconhecida, caso contrário não.

- **Armazenamento dos Dados:** É necessário armazenar em um banco de dados os templates e outras informações acerca do usuário. Dependendo da aplicação, o template pode ser armazenado em um local de armazenamento interno ou externo, ou ser gravado em cartão inteligente (*smart card*) que será entregue ao indivíduo.

A variabilidade que ocorre em um vetor de características originados de uma mesma classe é denominada variação intraclasse, e a variação entre vetores de características originados de duas classes diferentes é chamado de variação interclasse. Assim, para uma característica biométrica apresentar um bom resultado ela deve possuir um pequena variação intraclasse e uma grande variação interclasses.

O grau de similaridade entre dois vetores de características é medido por meio de uma pontuação ou *score* de similaridade. Uma pontuação de casamento é considerada

genuína ou autêntica se for resultado do casamento de duas amostras da mesma característica biométrica, e conhecida como pontuação impostora se envolver a comparação de duas amostras originadas de diferentes características biométricas. Uma pontuação impostora que excede um limiar ou *threshold* resulta em uma falsa aceitação, enquanto uma pontuação genuína que fica abaixo do *threshold* resulta em uma falsa rejeição. Seguindo este raciocínio, temos duas medidas principais para avaliar o desempenho de um sistema biométrico:

- **Taxa de Falsa Aceitação (*False Acceptance Rate* (FAR) ou *False Match Rate* (FMR)):** probabilidade de duas imagens de indivíduos diferentes serem classificadas como semelhantes, ou seja, a probabilidade de se aceitar um indivíduo impostor, calculada comparando cada template de um indivíduo com todos outros demais indivíduos da base de dados. Pode ser definida pela fração das pontuações de impostores que excederam o *threshold*.

- **Taxa de Falsa Rejeição (*False Rejection Rate* (FRR) ou *False Non-Match Rate* (FNMR)):** probabilidade de duas imagens da mesma característica de um indivíduo serem classificadas como diferentes, ou seja, a probabilidade de rejeitar um indivíduo genuíno, calculada comparando cada template de um indivíduo como todos os outros templates da mesma característica biométrica do mesmo indivíduo. Pode ser definida pela fração de pontuações de genuínos que ficaram abaixo do *threshold*.

Essas taxas podem ser melhor compreendidas por meio da visualização das distribuições das pontuações obtidas dos casamentos genuínos e impostores, conforme ilustra a Figura 2.14 (a).

Conforme pode ser visto na Figura 2.14(a), se aumentarmos o valor do limiar aumenta-se a taxa FRR, tornando o sistema mais inflexível a variações intraclasse. Por outro lado, se diminuirmos o valor do limiar, temos uma diminuição da taxa FRR, permitindo uma maior variabilidade intraclasse dos usuários, porém temos um aumento da taxa FAR, tornando o sistema menos seguro.

Os requisitos de segurança de um sistema biométrico dependem muito de cada aplicação. Por exemplo, em uma aplicação forense de identificação criminal, um dos problemas mais críticos é a FRR e não a FAR, pois neste caso não se pode perder a identificação de um criminoso, mesmo correndo o risco de examinar manualmente um número grande de suspeitos gerados incorretamente pelo sistema. No outro extremo, a taxa FAR talvez seja um dos fatores mais importantes em uma aplicação de controle

de acesso de alta segurança, onde o primeiro objetivo é deter impostores. Existem também algumas aplicações civis onde os requisitos de desempenho encontram-se entre os dois extremos, onde FAR e FRR devem ser considerados, por exemplo, em um caixa eletrônico bancário, caso um impostor seja aceito isso pode significar uma perda de dinheiro, enquanto uma taxa FRR alta pode levar a uma perda potencial de um cliente valioso (Jain & Maltoni, 2009). A Figura 2.14(b) ilustra as taxas FAR e FRR em diferentes tipos de aplicações biométricas.

A partir das taxas FAR e FRR pode-se extrair uma medida única para caracterizar o nível de segurança de um sistema biométrico, esta medida é a *Equal Error Rate* (EER), que representa a taxa de erro de um sistema biométrico para um limiar onde as taxas FAR e FRR possuem o mesmo valor.

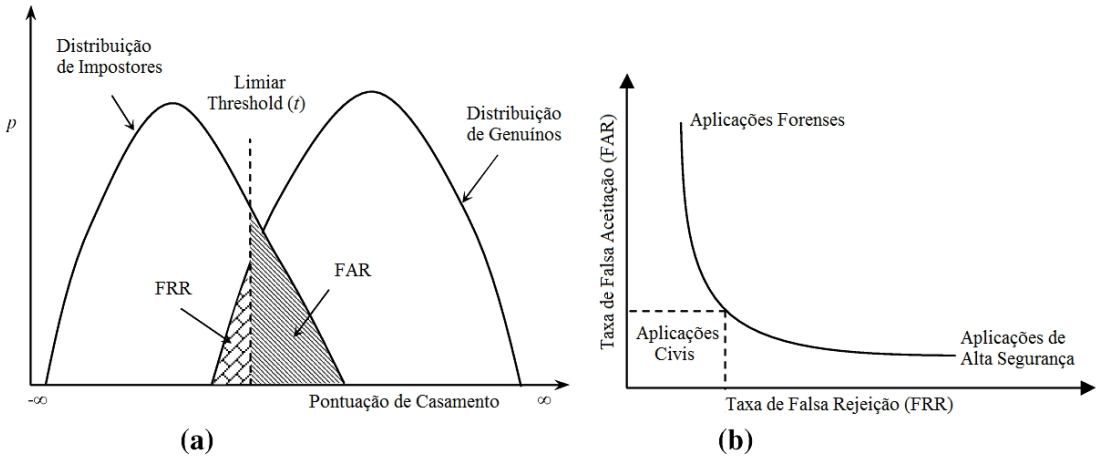


Figura 2.14: Taxas de erros em sistemas biométricos. (a) FAR e FRR para um limiar t são apresentadas para a distribuição de genuínos e impostores; FAR é o percentual de impostores que tiveram a pontuação maior que o limiar t e FRR é o percentual de genuínos que tiveram a pontuação menor que o limiar t. (b) Escolhendo diferentes limiares resulta em diferentes taxas FAR e FRR. A curva relativa as taxas FAR e FRR para diferentes limiares é denominada *Receiver Operating Characteristics* (ROC). Adaptado de (Jain et al., 2004).

2.5 Ataques a Sistemas Biométricos

A definição de um sistema biométrico seguro é difícil pois sistemas biométricos trazem novos conceitos que o diferenciam da computação tradicional e da segurança criptográfica (Jain et al., 2008).

Apesar do investimento em tecnologia e segurança em sistemas biométricos, principalmente os baseados em impressões digitais, ainda existem muitas vulnerabilidades que podem ser exploradas por pessoas mal intencionadas, para invadir estes sistemas ou simplesmente deixá-los fora de operação. Assim, além de investir em novas técnicas para melhorar as taxas de reconhecimento biométrico e tornar os sistemas mais robustos, também deve existir um forte investimento em técnicas e tecnologias que proporcionem maior segurança para estes sistemas.

Todo sistema biométrico é concebido visando aumentar a segurança na identificação de pessoas. Nestes sistemas, a ideia que se tem é que a utilização de uma característica biométrica, que é individual e não pode ser transferida a outra pessoa, caracteriza-se, por si só, como uma segurança para o sistema. Porém, esta linha de raciocínio não é correta, visto que existem vulnerabilidades que podem ser exploradas em sistemas biométricos. Estas vulnerabilidades surgem com a utilização de biometria, uma vez que sistemas de identificação baseados em posse ou conhecimento já têm suas vulnerabilidades bem definidas e estratégias para procurar minimiza-las. Com o aumento da utilização de biometria para identificação de pessoas em larga escala, novas vulnerabilidades podem surgir, necessitando, assim, de um esforço continuo em pesquisas para criar mecanismos de segurança.

Pode-se afirmar que nenhum sistema é totalmente seguro. Mas, isso não quer dizer que os sistemas biométricos não são desenvolvidos para serem melhor contra os possíveis ataques. O que vai definir o nível de segurança implementado são os requisitos de segurança necessários para o sistema. De acordo com Jain & Maltoni (2009), um modelo de segurança é baseado em o que você precisa proteger e de quem, levando em consideração os possíveis ataques já conhecidos. Desta forma, os diferentes tipos de sistemas e tipos de usos é que vão definir quais são as técnicas de segurança necessárias para proteger os dados e acessos ao sistema.

Os objetivos principais que motivam um ataque a um sistema são: derrubá-lo e deixá-lo inoperante, corromper a base de dados, adquirir dados sigilosos, obter privilégios de outra pessoa, esconder a sua própria identidade. Estes objetivos podem ser tanto de interesses pessoais, quanto para questões maiores, visando comprometer o próprio sistema.

Segundo Biggio et al. (2012), há poucos anos atrás, vulnerabilidades potencias em sistemas biométricos e ataques foram detectados, e alguns trabalhos revelaram que não apenas os módulos do sistema podem ser atacados, mas também os canais de comunicação utilizados por eles.

Possuir uma autenticação confiável tem-se tornado um requisito importante no mundo atual baseado em Internet. As consequências de um sistema de autenticação inseguro em uma corporação ou empresa podem ser catastróficas, e podem resultar na perda de dados confidenciais, bloqueio de serviços e comprometimento da integridade dos dados (Ratha et al., 2001).

Os sistemas biométricos possuem diversos pontos de vulnerabilidade, de acordo com a sua estrutura, e esses pontos podem ser atacados utilizando estratégias diferentes baseadas no objetivo do ataque. Para cada tipo de ataque devem ser adotadas técnicas diferentes de contramedida procurando minimizar os riscos de ataque.

Neste sentido Ratha et al. (2001) identificaram oito pontos em um sistema biométrico genérico onde ataques podem ocorrer, conforme ilustra a Figura 2.15. São eles:

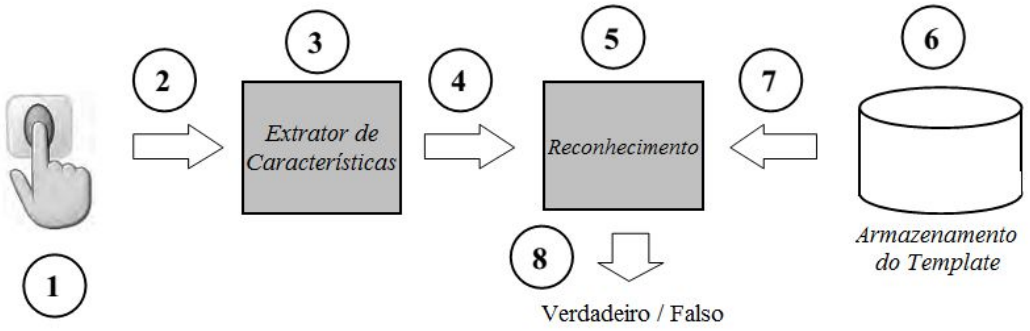


Figura 2.15: Pontos de ataque de um sistema biométrico. Adaptado de (Jain & Maltoni, 2009) e (Ratha et al., 2001).

1. Apresentar uma falsa biometria ao sensor: neste modo de ataque uma reprodução da biometria é apresentada ao sensor do sistema, como por exemplo uma impressão digital falsa, a cópia de uma assinatura ou uma foto de uma face;

2. Reenviar um sinal biométrico previamente digitalizado e armazenado: neste modo de ataque, um sinal armazenado é reenviado ao sistema, sem passar pelo sensor, como por exemplo, a apresentação de uma cópia antiga de uma imagem de impressão digital ou um sinal de áudio previamente gravado;

3. Sobrescrever o módulo de extração de características: neste modo de ataque o módulo de extração de características é atacado utilizando uma espécie de

vírus de computador denominado “Cavalo de Tróia”, que produz vetores de características pré-selecionados pelo invasor;

4. Adulterar a representação biométrica: neste modo de ataque as características extraídas do sinal de entrada são substituídas por uma diferente, geralmente por um vetor de características fraudulento. Em alguns casos os módulos de extração de características e de reconhecimento são acoplados, tornando este modo de ataque extremamente difícil de se praticar. Apesar disso, se um vetor de minúcias é transmitido pela Internet para um módulo de reconhecimento remoto, este tipo de ameaça é muito facilitado. Um “espião” pode, neste caso, alterar pacotes que trafegam sobre o protocolo *Transmission Control Protocol/Internet Protocol* (TCP/IP);

5. Corromper o módulo de reconhecimento: neste tipo de ataque o módulo de reconhecimento pode ser atacado e corrompido, gerando, assim, apenas scores pré-selecionados;

6. Adulterar templates armazenados: neste tipo de ataque o banco de dados de templates pode estar em uma infraestrutura local ou remota, e os dados podem estar distribuídos por vários servidores. Assim um invasor poderia modificar um ou vários templates armazenados na base de dados, o que poderia resultar tanto na autorização de um impostor, quanto, na negação de serviço para uma pessoa que teve seu template corrompido. Sistemas baseados em *smartcards*, onde o template é armazenado no próprio cartão e apresentado para o sistema de autenticação, são muito vulneráveis a este tipo de ataque;

7. Atacar o canal de comunicação entre a base de dados e o módulo de reconhecimento: neste tipo de ataque os templates são enviados para o módulo de reconhecimento através de um canal de comunicação e esses dados trafegando por este canal podem ser interceptados e modificados;

8. Sobrepor a decisão final: neste tipo de ataque se a decisão final do módulo de reconhecimento for sobreposta por um *hacker*, então todo o sistema de identificação pode ser desabilitado, uma vez que mesmo se o módulo de reconhecimento tiver uma excelente performance isto se torna irrelevante pelo simples fato de que a decisão será sobreposta no final.

Jain & Maltoni (2009) ressaltam dois tipos de falhas que podem ocorrer em sistemas biométricos que estão diretamente ligadas às questões de segurança: bloqueio de

acesso e intrusão. O bloqueio de acesso (*Denial of Service* (DoS)) é uma falha de acesso ao sistema, onde um usuário autorizado é bloqueado e não pode utilizar o serviço. A intrusão refere-se a uma pessoa não autorizada conseguir acesso ao sistema, depois de conseguir o acesso o *hacker* pode modificar algum dado ou simplesmente ter acesso a dados privilegiados ou confidenciais.

2.5.1 Ataques em Sistemas Biométricos Baseados em Impressões Digitais

Apresentar uma biometria falsa ao sensor é um dos tipos de ataque mais comuns em sistemas biométricos. Esse tipo de ataque é conhecido como *spoofing*. No caso de impressões digitais, este tipo de ataque pode ser realizado simplesmente apresentando ao sensor uma impressão digital construída artificialmente, ou então, utilizando um dedo desmembrado ou de um cadáver (Jain et al., 2008).

O primeiro ataque a um sistema biométrico baseado em impressões digitais aconteceu na década de 1920, quando um presidiário da penitenciária do Kansas usou sua experiência em fotografia e gravura para forjar impressões digitais latentes. A impressão digital foi fotografada, depois o negativo foi utilizado para gravar a impressão em uma placa de cobre levemente lubrificada, por último a placa foi utilizada para deixar impressões digitais falsas em objetos (Jain & Maltoni, 2009).

Mais recentemente, Matsumoto et al. (2002) mostraram que com dedos artificiais confeccionados com material flexível foi possível burlar com certa facilidade a maioria dos sensores de impressões digitais disponíveis na época. Na Figura 2.16 é possível visualizar o molde e o *spoof* criados para os testes realizados por Matsumoto et al. (2002).

Existem dois modos para se confeccionar um dedo artificial, o modo cooperativo e o não cooperativo (Coli et al., 2007).

No modo cooperativo ou consensual, a pessoa coloca seu dedo em um material maleável como, por exemplo, material para molde dentário, silicone, massa de modelar, argila ou cera, criando um molde. Em seguida, preenche-se o molde com materiais que contêm as mesmas propriedades da pele humana como, por exemplo, silicone, gelatina, massa de modelar, látex, entre outros. Se este processo for bem feito pode produzir uma réplica onde o padrão de cristas, minúcias e textura são bastante semelhantes ao dedo original (Marcialis et al., 2010).

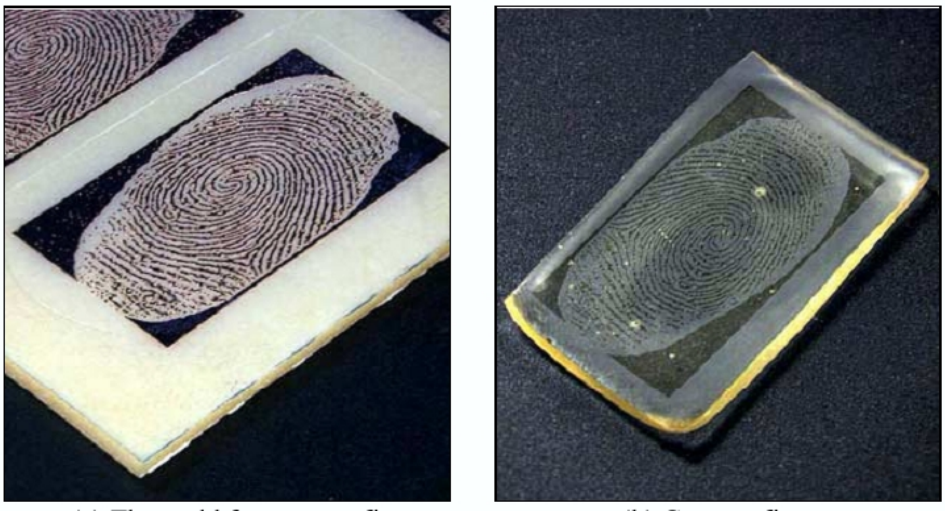


Figura 2.16: Fotografia da aparência externa do molde e do dedo de goma. O dedo de goma foi produzido a partir de uma impressão digital latente deixada em uma placa de vidro e melhorada utilizando uma cola (Matsumoto et al., 2002).

A Figura 2.17 (a) mostra uma fotografia do molde confeccionado com massa de modelar e a Figura 2.17 (b) o *spoof* criado a partir do molde com látex. Na Figura 2.18 são mostradas seis fotografias sobre o processo de fabricação passo a passo de um *spoof* de gelatina também de forma consensual.

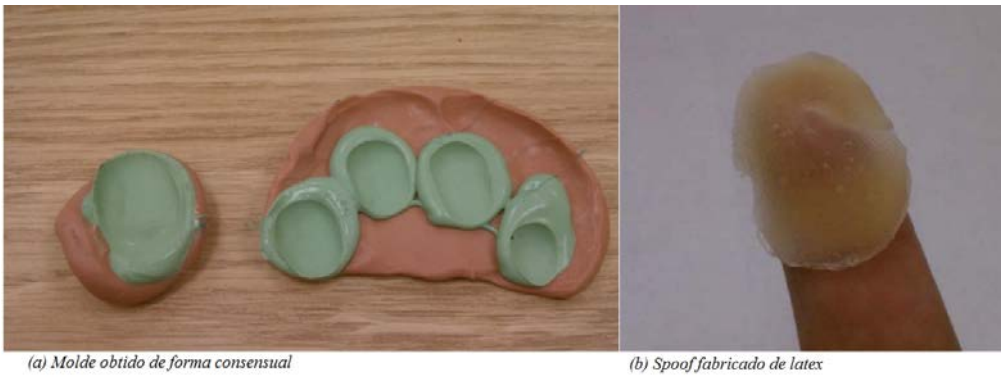


Figura 2.17: Processo de fabricação de um dedo falso (*spoof*). (a) Fotografia do molde obtido de forma consensual com massa de modelar. (b) *Spoof* fabricado com látex. Adaptado de (Yambay et al., 2012).

No método não-cooperativo, produz-se uma impressão digital falsa a partir de uma impressão digital latente, deixada pelo indivíduo alvo ao tocar com os dedos uma superfície lisa. Este método é mais complexo e requer maior conhecimento sobre as técnicas utilizadas por peritos forenses. Além disso, a qualidade das

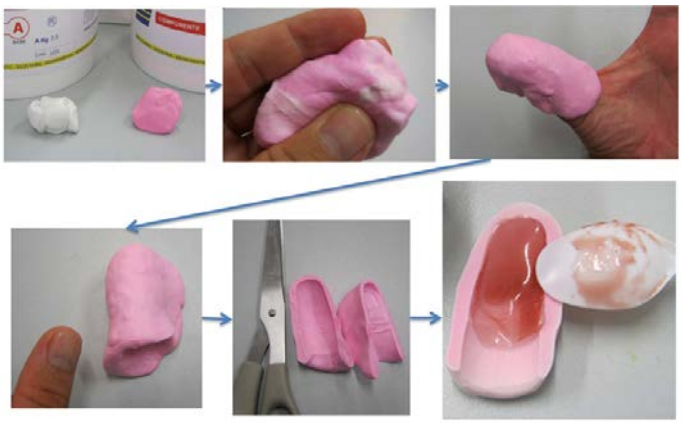


Figura 2.18: Processo de fabricação de um dedo falso (*spoof*) (Ghiani et al., 2013).

impressões digitais obtidas é bem pior do que as impressões obtidas através do método cooperativo (Coli et al., 2007).

Para confeccionar um *spoof* a partir de uma impressão digital latente primeiramente a impressão digital deixada em alguma superfície passa por um processo de melhoramento, depois ela é digitalizada utilizando uma máquina fotográfica, e por último o negativo da imagem é impresso em uma folha de transparência. Esta imagem impressa pode, então, ser colocada dentro de um molde, como por exemplo, a gravação da imagem sobre uma placa de circuito impresso que pode ser utilizado para criar o molde de criação do *spoof* (Ghiani et al., 2013). A Figura 2.19 mostra os passos para criação de um *spoof* utilizando o método não-cooperativo.

2.6 Considerações Finais

Neste capítulo foi introduzido o conceito de Biometria, apresentados exemplos das principais características biométricas humanas que podem ser utilizadas para o reconhecimento e os requisitos que estas características devem atender, depois, conceitos relacionados às impressões digitais foram explorados, mostrando as principais características das impressões digitais que estão divididas em três níveis e os tipos de sensores que podem ser utilizados para capturar as impressões digitais. Em seguida foram apresentadas as taxas de erros utilizadas para avaliação dos sistemas biométricos, como a FAR, FRR e a EER. Na sequencia foram apresentados os tipos de ataques que podem ocorrer em sistemas biométricos de uma forma geral, desde ataques a nível de sensor até os ataques a nível de rede e algoritmo. Por fim, foram

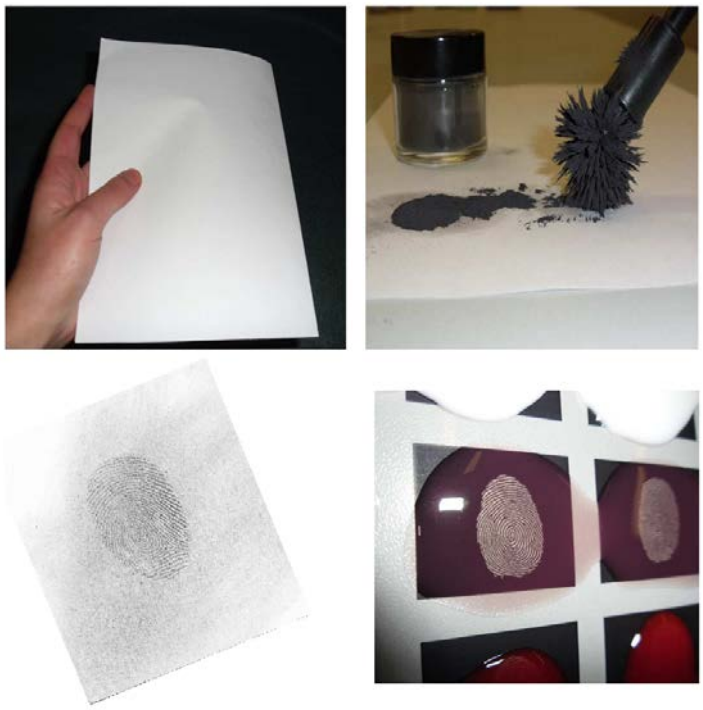


Figura 2.19: Processo de criação de uma impressão digital falsa (*spoofing*) pelo modo não cooperativo. Adaptado de (Ghiani et al., 2013).

descritos os ataques em sistemas biométricos baseados em impressões digitais com foco nos ataques do tipo *spoofing*.

Capítulo 3

Métodos para Detecção de Impressões Digitais Falsas

Recentemente, pesquisadores têm dedicado grande atenção para sistemas biométricos devido a importância das aplicações e seus desafios, e alguns deles mostraram que tais sistemas são vulneráveis a ataques no nível do sensor, em particular os sistemas de reconhecimento de impressões digitais. Matsumoto et al. (2002) criaram dedos de gelatina e estudaram ataques do tipo *spoofing* em onze sistemas comerciais baseados em impressões digitais, com sensores ópticos e capacitivos. Os experimentos mostraram que 100% desses sistemas aceitaram o cadastramento de dedos falsos que também foram posteriormente aceitos na etapa de verificação, com uma alta probabilidade (68-100% para dedos confeccionados de forma cooperativa e 67% para dedos confeccionados de forma não cooperativa).

Desse modo, o desenvolvimento de métodos eficientes para proteger estes sistemas desse tipo de ataque é urgente. Para tanto, podemos utilizar técnicas para verificar a vivacidade de uma impressão digital apresentada ao sensor utilizando soluções de *hardware* ou de *software*. O trabalho desenvolvido por Al-Ajlan (2013) apresenta uma visão geral do "estado da arte" no que diz respeito às técnicas de detecção de impressões digitais falsas. Dentre as principais técnicas abordadas, as que utilizam características de terceiro nível, como os poros ou o padrão de transpiração, são bastante promissoras, conforme ilustra a Figura 3.1. Inspirados pelo trabalho de Al-Ajlan (2013), nossos estudos também estão focados nos métodos *antispoofing* baseados em *software* e que utilizam características de terceiro nível, principalmente os poros sudoríparos.

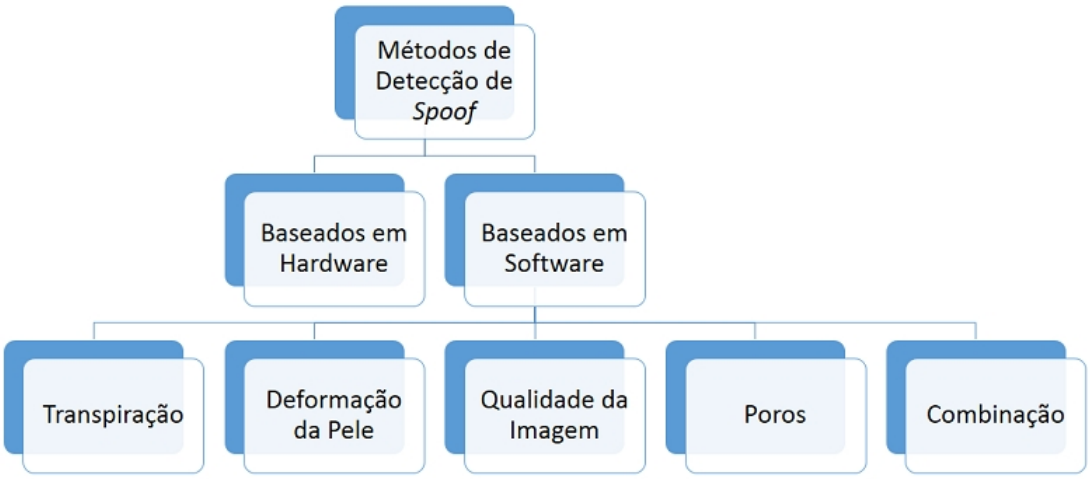


Figura 3.1: Estado da arte das pesquisas de métodos de detecção de *spoof*. Adaptado de (Al-Ajlan, 2013) .

A subdivisão dos métodos de detecção de *spoof* baseados em *software* depende dos tipos de recursos utilizados. Se as características extraídas forem derivadas de múltiplos frames da mesma imagem capturados enquanto uma pessoa coloca o dedo na superfície do sensor por um certo período, como por exemplo, dois frames capturados com 0 e 5 segundos, este método é chamado de "dinâmico", pois utiliza características dinâmicas. Por outro lado, se as características extraídas forem de uma única impressão digital ou da comparação de diferentes impressões digitais, o método é chamado "estático", pois utiliza características estáticas (Coli et al., 2007).

Na Tabela 3.1 temos um comparativo entre os principais métodos que utilizam características de terceiro nível.

3.1 Métodos Baseados em Padrão de Transpiração

A pele humana é formada por três camadas principais, sendo que a camada periférica contém cerca de 600 glândulas sudoríparas por centímetro quadrado. O suor, uma solução diluída de cloreto de sódio, é difundido na superfície da pele através de pequenos poros, que não desaparecem e não se alteram com o decorrer do tempo. Observações mostram que a distância entre os poros é de aproximadamente 0.5 mm na ponta do dedo.

Tabela 3.1: Comparativo entre métodos de detecção de *spoofing* em impressões digitais.

Método	Técnica	Resolução	Sensor	Abordagem	Base de Dados	Forma de Coleta
(Marcialis et al., 2010)	Poros	569dpi	Óptico	Dinâmica Estática	Própria	Consensual
(Parthasaradhi et al., 2005)	Transpiração	NI	Capacitivo Óptico	Dinâmica Estática	Própria	Consensual Não Consensual
(Choi et al., 2007)	Histograma	500dpi	Óptico	Estática	Própria	Consensual
(Galbally et al., 2012)	Qualidade	500dpi	Óptico	Estática	LivDet2009	Consensual Não Consensual
(Espinoza & Champod, 2011)	Poros	1000dpi	Óptico	Dinâmica	Própria	Consensual
(Nikam & Agarwal, 2008)	Textura	500dpi	Óptico	Estática	Própria	Consensual
(Derakhshani et al., 2003)	Transpiração	NI	Capacitivo	Dinâmica Estática	Própria	Consensual
(Ghiani et al., 2012)	Textura	500dpi	Óptico	Estática	LivDet2011	Consensual Não Consensual
(Pereira et al., 2012)	Histograma Transpiração	NI	NI	Estática	Própria	Consensual
(Cavalcanti et al., 2012)	Histograma Transpiração	NI	NI	Estática	Própria	Consensual
(Marasco & Sansone, 2010)	Histograma Transpiração	500dpi	Óptico	Estática	LivDet2009	Consensual

Derakhshani et al. (2003), por meio de experimentos realizados com impressões digitais de dedos com vida, de impressões digitais artificiais e impressões digitais de cadáveres, relataram algumas observações acerca do fenômeno fisiológico que acontece quando uma impressão digital é capturada utilizando-se um sensor:

1. Em impressões digitais com vida a transpiração inicia nos poros, cobrindo-os completamente, ou deixando-os como um ponto seco no centro da fonte de transpiração. Normalmente a primeira impressão digital capturada parece irregular devido a este processo de transpiração, esta propriedade formou a base para a abordagem estática de classificação. Na Figura 3.2(a) é possível perceber esta propriedade;

2. Com o tempo, o suor se difunde ao longo das cristas, tornado úmidas as regiões semi-secas entre os poros e, consequentemente, fazendo com que as imagens das impressões digitais fiquem mais escuras nessas regiões. Exceto se a pele for extremamente seca, a região do poro permanece saturada, enquanto a umidade gerada pelo suor se espalha para as partes mais secas conforme mostra a Figura

3.2 (a). Esta propriedade pode ser observada comparando-se as duas imagens capturadas dentro de 5 segundos e serve de base para a abordagem dinâmica;

3. Obviamente, o processo de transpiração não ocorre nos dedos artificiais e nos dedos de cadáveres. Portanto, esse efeito causado pela transpiração em imagens de dedos vivos não pode ser observado em imagens capturadas a partir de dedos de um cadáver ou de um dedo artificial, conforme mostram as Figuras 3.2 (b) e 3.2 (c).

Assim a base do método proposto por Derakhshani et al. (2003), e melhorado por Parthasaradhi et al. (2005), é simples e direta. Impressões digitais capturadas de dedos com vida, ao contrário das impressões capturadas de cadáveres e *spoof*, apresentam mudanças temporais devido ao fenômeno fisiológico da transpiração, que podem ser capturadas pelos *scanners* comerciais (ópticos, capacitivos ou ultrassônicos).

O desafio do algoritmo de processamento de imagem é quantificar o padrão de transpiração, além disso, sendo a transpiração um fenômeno fisiológico este padrão pode variar de pessoa para pessoa, podendo influenciar na quantidade de umidade inicial contida na pele.

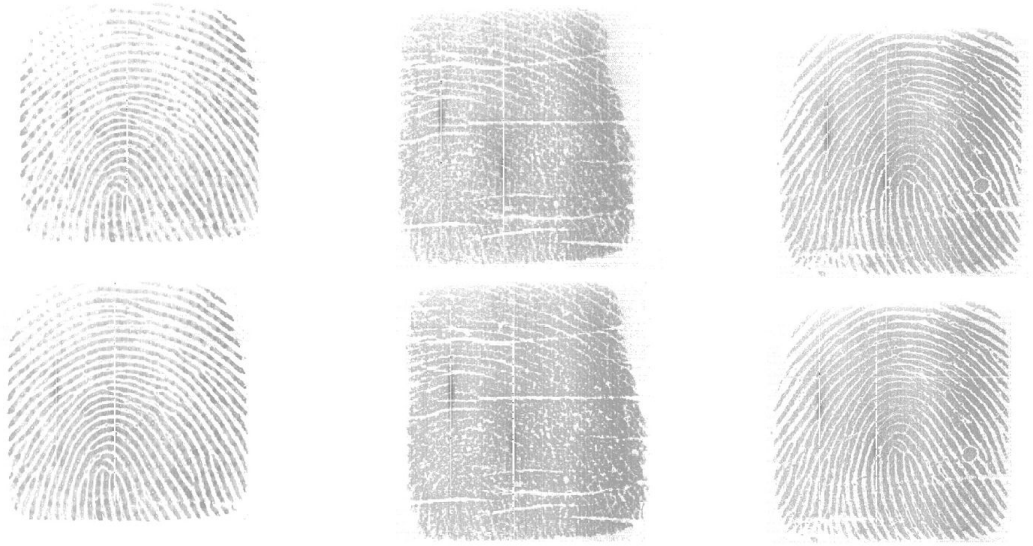


Figura 3.2: Exemplos de impressões digitais, capturadas com 0 segundo (superior) e 5 segundos (inferior). (a) Impressão digital de dedo com vida, (b)Impressão digital de dedo de um cadáver e (c) Impressão digital de dedo falso (*spoof*). Adaptado de (Derakhshani et al., 2003)

Para quantificar o fenômeno de transpiração em uma sequência temporal de imagens um algoritmo foi desenvolvido para mapear uma imagem de impressão digital bidimensional em um sinal que representa os níveis de cinza no decorrer das cristas conforme é mostrado na Figura 3.3.

Neste algoritmo, a última imagem capturada é utilizada para determinar a localização das cristas, uma vez que normalmente as cristas estão mais escuras proporcionando um melhor resultado. As variações nos níveis de cinza no sinal correspondem às variações na umidade que pode ser medida estaticamente quando utilizamos apenas uma imagem ou dinamicamente quando é calculada a diferença entre duas imagens capturadas consecutivamente. A característica estática mede a variação periódica nos níveis de cinza no decorrer das cristas devido a presença da transpiração ao redor dos poros, nesta medida, as pequenas áreas, altamente hidratadas ao redor dos poros sudoríparos (e não os próprios poros) são detectadas como um sinal de transpiração ativa e, portanto, de vivacidade.

As características dinâmicas, por sua vez, quantificam as mudanças temporais no sinal das cristas devido a propagação da umidade entre os poros da imagem inicial em relação a imagem capturada 5 segundos depois, onde em dedos com vida os níveis de transpiração nas áreas ao redor dos poros permanecem saturados e quase inalterados, enquanto, as áreas mais secas das cristas entre os poros mostram um aumento no nível de transpiração. Nos dedos de cadáver e *spoof* não são observados os padrões estático e dinâmico devido à ausência de transpiração ativa (Parthasaradhi et al., 2005).

O algoritmo proposto por Derakhshani et al. (2003) executa 13 passos principais que envolvem a captura, o pré-processamento, a extração das medidas e a classificação:

1. Capturar um par consecutivo de impressões digitais em um intervalo de 5 segundos;

2. Processar as impressões digitais para remover ruídos e defeitos de captura, utilizando um procedimento de redução de ruído e o filtro da mediana;

3. Obter a versão binarizada da última imagem;

4. Afinar a imagem binarizada para que as cristas fiquem com apenas um pixel de largura. Ajustar o resultado para que as cristas afinadas passem pelo meio das cristas originais;

5. Remover bifurcações para que os contornos fiquem como curvas individuais;

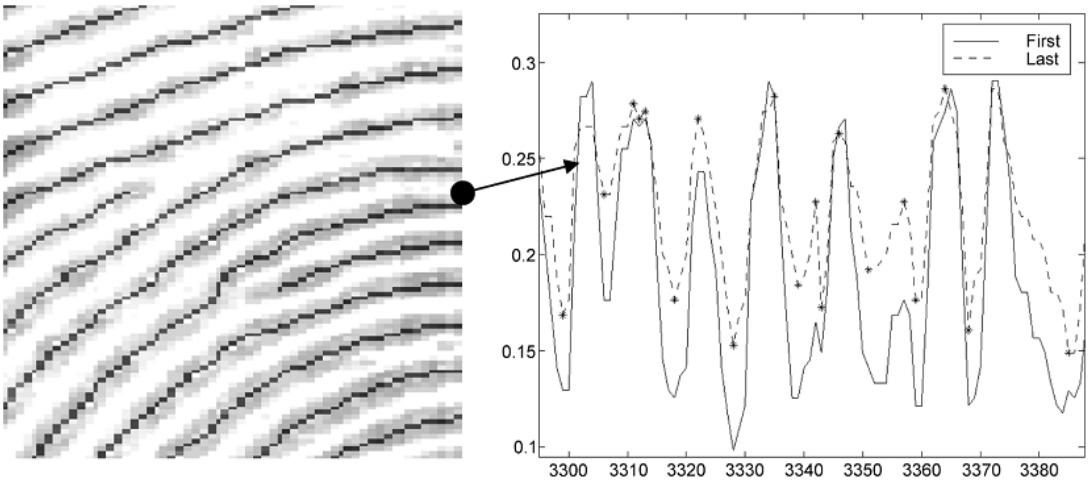


Figura 3.3: Mapa de cristas sobreposto na impressão digital original (esquerda) e resultado do sinal para as duas imagens capturadas, em 0 segundo (linha sólida) e em 5 segundos (linha tracejada). Adaptado de (Parthasaradhi et al., 2005).

6. Retirar dois pixels das extremidades dos contornos e descartar curvas menores de 15 pixels;

7. Utilizar as curvas obtidas no passo 6 como uma máscara e converter os níveis de cinza ao longo delas em sinais para a primeira e última imagens, conforme ilustra a Figura 3.3;

8. Calcular a Transformada de Fourier do sinal gerado para a primeira imagem no passo 7 e sua média. Calcular a energia total que corresponde ao espaço de frequência de poros (esta medida é uma característica estática);

9. Conectar os sinais obtidos no passo 7 para a primeira e última imagens e formar longos sinais que representarão cada impressão digital (C1, C2);

10. Detectar os máximos e mínimos locais dos sinais da primeira e última imagens;

11. Calcular uma série de parâmetros para quantificar o processo de transpiração (essas medidas são características dinâmicas);

12. Armazenar os resultados e processar as características selecionadas;

13. Tomar uma decisão sobre a vivacidade utilizando um classificador neural.

O trabalho publicado por Derakhshani et al. (2003) estabelece ainda cinco medidas que podem ser utilizadas para detecção de vivacidade em impressões digitais, sendo uma medida estática e quatro medidas dinâmicas:

- **SM - Medida Estática – Energia (Uniformidade):** A medida estática utiliza a média da transformada de Fourier do sinal obtido a partir dos tons de cinza da primeira imagem para quantificar a existência de poros ativos, onde a energia relacionada com o espaçamento típico dos poros é utilizado. Uma FFT é realizada e o total da energia é avaliada para uma distância de 8 a 24 pixels (para um espaçamento de poros padrão de 0.4 a 1.2mm) que leva em conta o caso da falta de um poro com um espaçamento máximo de 0.6mm. Isto corresponde a faixa de frequência de espaço entre 11 e 33 (número de pontos da FFT pontos/período espacial). Antes de efetuar a FFT, a fim de eliminar o pico de frequência em torno de zero, a corrente contínua do sinal é removida apenas para efeitos de cálculo. O procedimento pode ser expresso matematicamente como:

$$SM = \sum_{k=11}^{33} f(k)^2 \tag{3.1}$$

onde

$$f(k) = \frac{\sum_{i=1}^{n} \left| \sum_{p=1}^{255} S_{1i}^{a}(p) e^{-j2\pi(k-1)(p-1)/256} \right|}{n}$$

$S_{1i}^{a} = S_{1i} - média(S_{1i})$, onde n é o número total de cristas obtidas no passo 6 e S_{1i} são as cristas individuais da primeira imagem.

- **DM1 - Medida Dinâmica 1 - Oscilação total entre as imagens:** Em geral, na primeira imagem temos poros úmidos e regiões secas entre eles fazendo com que a imagem contenha uma maior variação dos níveis de cinza, já na última imagem o suor já se espalhou para regiões mais secas, assim teremos uma menor variação dos níveis de cinza. Em termos matemáticos, a primeira medida dinâmica é representada por:

$$DM1 = \frac{\sum_{i=1}^{m} |C_{1i} - C_{1i-1}|}{\sum_{i=1}^{m} |C_{2i} - C_{2i-1}|} \tag{3.2}$$

onde C_{1i} e C_{2i} referem-se ao sinal que representa os tons de cinza da primeira e última imagem respectivamente e m o tamanho do sinal. O valor de m é o mesmo tanto para C_{1i} quanto para C_{2i}, uma vez que a mesma máscara foi utilizada para geração dos sinais.

- **DM2 - Medida Dinâmica 2 – Taxa máxima/mínima de crescimento:** Para uma impressão digital de um dedo verdadeiro os valores máximos do

sinal não aumentam tão rapidamente quanto os mínimos, visto que os poros sudoríparos já estão saturados. Em termos matemáticos, a medida dinâmica 2 (DM2) é descrita a seguir:

$$DM2 = \frac{\sum_j (C_{2j}^{min} - C_{1j}^{min})}{\sum_k (C_{2k}^{max} - C_{1k}^{max})} \tag{3.3}$$

onde C_{1j}^{min} e C_{2j}^{min} são os locais mínimos para a primeira e segunda imagens respectivamente e C_{1k}^{max} e C_{2k}^{max} são os máximos locais. As localizações dos máximos e mínimos locais foram determinadas a partir da análise da última imagem e aplicada na primeira e última imagens.

- **DM3 - Medida Dinâmica 3 – Diferença média entre as imagens:** Subtraindo a primeira imagem da última para impressões digitais geradas a partir de um *spoof* a diferença apresentada será menor do que para imagens geradas a partir de dedos com vida. Em termos matemáticos, a medida dinâmica 2 (DM2) é descrita sendo:

$$DM3 = \frac{\sum_{i=i}^{m} (C_{2i} - C_{1i})}{m} \tag{3.4}$$

onde m, C_{1i} e C_{2i} são os mesmos valores descritos na DM1.

- **DM4 - Medida Dinâmica 4 – Variação percentual dos desvios padrão:** O raciocínio por traz desta medida é similar aos demais. Partindo-se do princípio de que as imagens falsas não possuem o efeito fisiológico da transpiração e calculando-se o desvio padrão entre as duas imagens, espera-se que esta medida seja menor se comparada com impressões digitais geradas a partir de dedos com vida. Em termos matemáticos:

$$DM4 = \frac{SD(C_1) - SD(C_2)}{SD(C_1)} \tag{3.5}$$

onde SD é o operador do desvio padrão:

$$SD(C) = \sqrt{\frac{\sum_{i=1}^{m} (C_i - média(C))^2}{m-1}}$$

Os resultados para este método podem ser avaliados analisando cada medida individualmente. As taxas de erro igual (EER) para cada medida estão mostradas na Tabela 3.2.

Nenhuma das cinco medidas extraídas das impressões digitais sozinha pode distinguir entre impressões digitais com vida e *spoof*/cadáver com 100% de precisão. A combinação de todas estas medidas alcança melhores resultados. Uma rede neural *back-propagation* utilizando as cinco medidas alcançou 100% de precisão (Derakhshani et al., 2003).

Tabela 3.2: Taxa de erro igual (*Equal Error Rate* - EER) para cada medida apresentada. Adaptado de (Derakhshani et al., 2003).

Medida	EER(Com Vida X *spoof*)	EER(Com vida X Cadáver)
SM	11.11	5.56
DM1	22.22	27.78
DM2	11.11	22.22
DM3	16.67	38.89
DM4	22.22	27.78

A fim de melhorar este método, Parthasaradhi et al. (2005) introduziram duas novas medidas dinâmicas e efetuaram os testes utilizando uma base de dados mais diversificada que conta com impressões digitais latentes e uma gama maior de sensores. As novas medidas introduzidas foram:

- **DM5 - Medida Dinâmica 5 – Percentual de mudança da saturação seca:** Esta medida indica o quão rápido o sinal da crista da região baixa de corte (*low cutoff region*) está desaparecendo, assim, extraindo mais informações da taxa de transpiração da região baixa. Em termos matemáticos:

$$DM5 = \frac{\sum_{i=1}^{m} \delta(C_{1i} - LT) - \delta(C_{2i} - LT)}{0.1 + \sum_{i=1}^{m} \delta(C_{2i} - LT)} \tag{3.6}$$

  onde C_{1i} refere-se ao pixel i (pixel com tom de cinza) no primeiro sinal de cristas e C_{2i} é análogo para a segunda captura. O i varia de 1 ao tamanho do sinal das cristas m. LT é o limiar para a região baixa (*low-cutoff threshold*) do sinal de cristas ($min(C_i)$). δ é a função delta discreta. Um valor elevado para esta medida corresponde a um rápido desaparecimento da saturação seca, pois a transpiração aumenta na linha base do sinal da crista acima da região de corte baixa do sensor, indicando assim uma transpiração contínua.

- **DM6 - Medida Dinâmica 6 – Percentual de mudança da saturação molhada:** Esta medida indica o quão rápido o sinal da crista da região alta de

corte (*high cutoff region*) está aparecendo, assim, extraindo mais informações de transpiração da região de saturação molhada (*wet-saturation region*).

$$DM6 = \frac{\sum_{i=1}^{m} \delta(C_{1i} - HT) - \delta(C_{2i} - HT)}{0.1 + \sum_{i=1}^{m} \delta(C_{2i} - HT)} \tag{3.7}$$

onde C_{1i} e C_{2i} são iguais a DM5. HT é o limiar para a região alta (*high-cutoff threshold*) do sinal de cristas $max(C_i)$). δ é a função delta discreta. Um valor mais alto da medida DM6 indica o aparecimento rápido de umidade saturada, uma vez que a transpiração aumenta a linha base do sinal de cristas em direção aos níveis de saturação do sensor, indicando assim uma transpiração contínua.

3.2 Métodos Baseados em Estatísticas de Poros

Marcialis et al. (2010) desenvolveram um método para detecção de *spoofing* utilizando a distribuição de poros em impressões digitais. O método foi avaliado em uma base de dados com mais de 14.000 impressões digitais.

Atualmente, esta é a maior base de dados para detecção de vivacidade em impressões digitais. Este método pode ser aplicado para impressões digitais capturadas em diversos sensores com resolução superior a 500 dpi para que os poros possam ser detectados, o sensor utilizado para testar o método possui 569 dpi. Partindo do princípio que o tamanho dos poros é inferior a 1 mm, o processo de reprodução de uma impressão digital que contenha poros é muito difícil.

O método realiza os seguintes passos, ilustrados na Figura 3.5, para extração de características que serão utilizadas na detecção de vivacidade:

1. O indivíduo coloca o seu dedo real ou dedo artificial (*spoof*) na superfície do sensor, e duas imagens são capturadas na sequência, em 0 e 5 segundos. Enquanto o indivíduo mantém o dedo na superfície do sensor o dedo real transpira, permitindo a detecção de vida. Foi observado que, devido ao processo de transpiração, para um dedo real, a imagem capturada em 0 segundo possui uma definição menor do que a capturada com 5 segundos. Portanto, caso não ocorra uma diferença significativa entre as duas imagens, pode-se supor que o sensor está sob ataque e que o dedo apresentado é artificial, ou de um cadáver;

2. Poros são detectados nas duas imagens. Para tanto, é utilizado um template conforme mostra a Figura 3.4 (este template é baseado na aparência visual

dos poros). O processamento consiste em percorrer as cristas, e calcular uma medida denominada "distância de poro", ou seja, a distância entre a região e o template. Um limiar (*threshold*) definido manualmente é utilizado para decidir quando um poro é detectado. Devido a simplicidade do método, o algoritmo consegue uma boa performance com relação ao tempo de processamento, além de obter também bons resultados com relação à detecção;

3. O número de poros é computado para três regiões de interesse (*Region of Interest* (ROI)) ao redor do centro da impressão digital. As regiões de interesse são definidas como: um quadrado de 100 x 100, um quadrado de 160 x 160 pixels e a impressão digital inteira, assim temos três valores para cada frame. A diferença entre os valores correspondentes em 0 e 5 segundos é computada, essas diferenças correspondem as três primeiras características adotadas sendo chamadas PD100, PD160 e PDWHOLE (*Pore Diference* (PD)), estas características servem para analisar o padrão de transpiração;

4. A distância euclidiana é calculada entre os poros das imagens capturadas em 5 segundos, bem como a média para cada região de interesse. Estas medidas correspondem a três características, chamadas ED100, ED160 e EDWHOLE (*Euclidean Distance* (ED)). Estas características para impressões digitais de dedos com vida devem exibir valores menores do que as impressões falsas, dado que é esperado um número maior de poros em impressões digitais verdadeiras;

5. Um rótulo de qualidade é extraído utilizando o algoritmo NIST *Fingerprint Image Quality Measure* (NFIQ) gerando mais uma característica chamada Q.

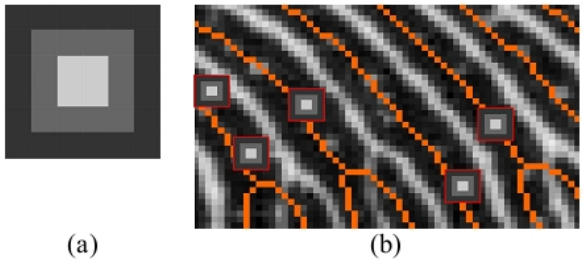


Figura 3.4: Template para detecção de poros. (a) Template. (b) Exemplo de detecção de poros utilizando o template. Adaptado de(Marcialis et al., 2010) .

Portanto, um vetor com sete características é gerado agrupando as sete medidas extraídas pelo algoritmo proposto: PD100, PD160, PDWHOLE, ED100, ED160, EDWHOLE e Q, conforme mostra a Figura 3.5.

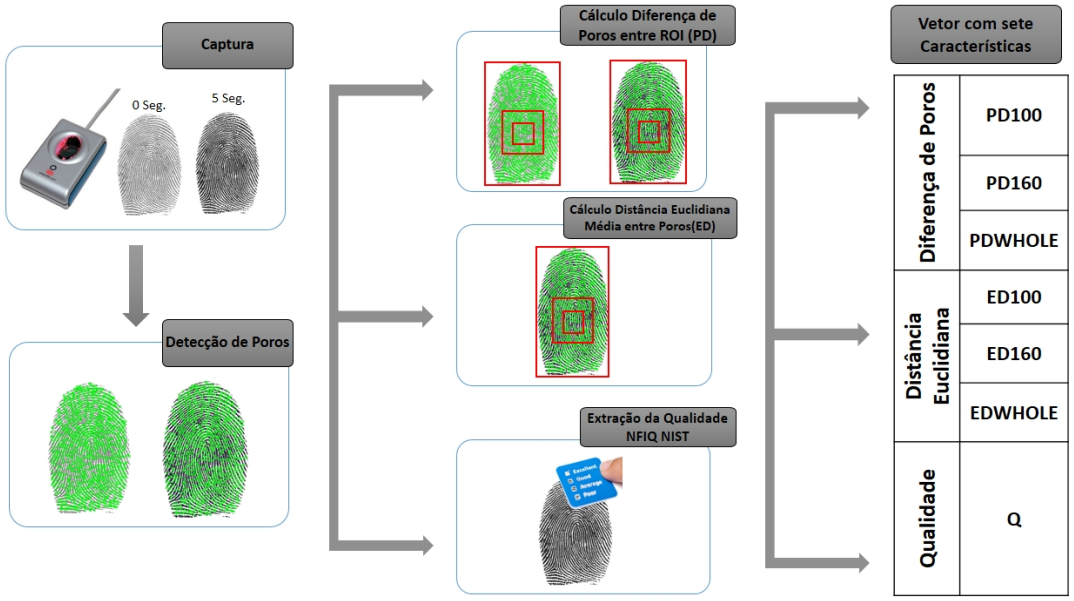


Figura 3.5: Processo de extração de características do método de detecção de impressões digitais falsas proposto por Marcialis et al. (2010).

Primeiramente, foi avaliada a capacidade discriminativa das características extraídas das impressões digitais. Os resultados dessa avaliação estão mostrados na Figura 3.6, sendo a Figura 3.6 (a) referente as impressões digitais de dedos com vida, e a Figura 3.6 (b) referente as impressões digitais de *spoof*. Os gráficos dessas figuras foram gerados a partir de 100 amostras aleatórias.

Devido ao fenômeno fisiológico da transpiração, pode-se notar que a quantidade de poros aumenta significativamente entre as imagens capturadas em 0 e 5 segundos de impressões digitais de dedos com vida. Por outro lado, nas imagens capturadas a partir de um *spoof* o número de poros não aumenta, para muitas amostras a diferença chega a ser negativa, indicando assim a ausência de transpiração. Além disso o número de poros, representado pelo eixo das ordenadas da Figura 3.6, é em média superior em impressões digitais verdadeiras. Outro fator importante que pode ser notado nos gráficos é que aumentando a região de interesse nas impressões digitais falsas e com vida, a dinâmica de diferença também aumenta de forma oposta, assim a diferença aumenta para impressões de dedos com vida e diminui para impressões de dedos falsos.

A performance da abordagem proposta por Marcialis et al. (2010) foi comparada com o método de características dinâmicas proposto por Parthasaradhi et al. (2005) que se baseia no efeito da transpiração, também foi feito uma combinação dos dois

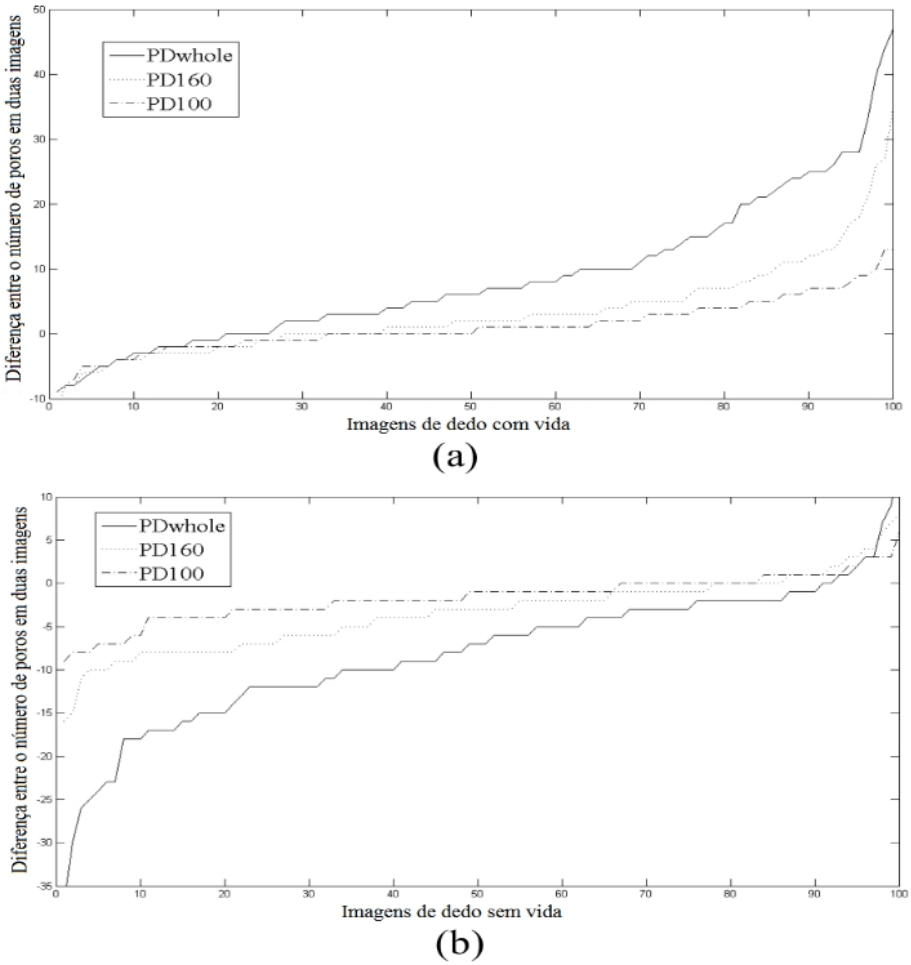


Figura 3.6: Características PD100, PD160 e PDWHOLE para 100 amostras aleatórias. (a) Impressões digitais de dedos com vida. (b) Impressões digitais de dedos sem vida. Adaptado de (Marcialis et al., 2010) .

métodos em um único vetor de características. A curva ROC apresentada na Figura 3.7 mostra os resultados obtidos. Pode-se observar que características extraídas de poros podem ser discriminativas para detecção de impressões digitais com vida e *spoof*. Esses resultados sugerem que réplicas de impressões digitais não conseguem reproduzir os detalhes de mais baixo nível como os poros, devido a limitações dos materiais disponíveis para moldar e confeccionar o *spoof*. Efetuando uma combinação entre o método baseado em poros e o método de características dinâmicas é possível melhorar o resultado final.

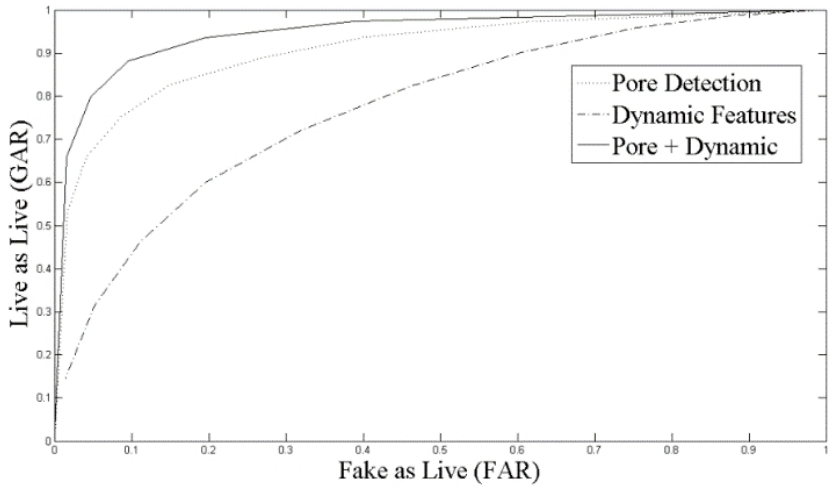


Figura 3.7: Curva ROC comparando abordagem de detecção de poros e características dinâmicas e sua fusão. Classificador K-NN foi utilizado. Resultados são uma média utilizando 10-fold cross-validation. Adaptado de(Marcialis et al., 2010) .

3.3 Métodos Baseados em Estatísticas de Primeira Ordem dos Tons de Cinza

Marasco & Sansone (2010) em seus estudos acerca de técnicas para detecção de impressões digitais falsas utilizam características extraídas dos histogramas das imagens, estas técnicas foram baseadas nos estudos prévios realizados por Tan & Schuckers (2005) e Abhyankar & Schuckers (2006), nos quais apontam que existe uma diferenciação entre os histogramas das imagens de acordo com a estrutura física da impressão digital. Assim sendo, por meio da utilização de índices estatísticos gerados a partir das distribuições dos histogramas, pode-se efetuar a classificação das amostras.

Este método efetua um pré-processamento em que as imagens passam pela equalização de histograma, que consiste em obter a máxima variância do histograma de uma imagem, obtendo assim uma imagem com melhor contraste. A equalização do histograma é realizada por meio de uma transformação T, que mapeia valores r de intensidade de uma imagem a ser processada em um nível de intensidade de saída s para todos os pixels de entrada:

$$s = T(r), onde : 0 \leq r \leq L - 1 \tag{3.8}$$

O L representa o número de tons de cinza avaliados pelo histograma e T é dada por:

$$S_k = T(r_k) = (L-1)\sum_{j=0}^{k} p_r(r_j) \tag{3.9}$$

Sendo $p_r(r_j)$ a probabilidade de ocorrência do nível de intensidade r_j em uma imagem digital.

As características expostas a seguir são dadas em função do histograma normalizado $H'(n)$ após a equalização realizada no pré-processamento:

$$H'(n) = \frac{H(n)}{MN} \tag{3.10}$$

onde $H'(n)$ é o histograma equalizado da imagem, M representa a altura e N a largura da imagem em pixels. A distinção entre uma impressão digital capturada de um dedo com e vida e uma dedo falso é baseada nas propriedades das estatísticas de primeira ordem, a saber (Abhyankar & Schuckers, 2006):

- Energia:

$$e = \sum_{n=0}^{N-1} H'(n)^2 \tag{3.11}$$

- Entropia:

$$S = -\sum_{n=0}^{N-1} H'(n) log H'(n) \tag{3.12}$$

- Mediana:

$$M = argmin_a \sum_{n} H'(n)\,|n-a| \tag{3.13}$$

- Variância:

$$\sigma^2 = \sum_{n=0}^{N} (n-\mu)^2 H'(n) \tag{3.14}$$

- Assimetria:

$$\gamma 1 = \frac{1}{\sigma^3} \sum_{n=0}^{N-1} (n - \mu)^3 H'(n) \tag{3.15}$$

- Curtose do Histograma:

$$\gamma 2 = \frac{1}{\sigma^4} \sum_{n=0}^{N-1} (n - \mu)^4 H'(n) \tag{3.16}$$

- Coeficiente de Variação:

$$cv = \frac{\sigma}{\mu} \tag{3.17}$$

onde N é igual ao número de tons de cinza, μ é a média e σ o desvio padrão.

Além das características extraídas a partir de estatísticas de primeira ordem, Tan & Schuckers (2005) e Marasco & Sansone (2010) propuseram mais duas medidas que se baseiam no contraste entre regiões mais claras e escuras em função do histograma relativo ao sinal das cristas. Sendo que do ponto de vista de distribuição de intensidade, entre as 256 diferentes intensidades possíveis, as imagens de impressões digitais falsas e de cadáveres possuem pixels com uma distribuição mais escura, ou seja, com seus valores menores do que 150. Seguem duas medidas de intensidade:

- **Níveis de Cinza 1**: Correspondente à relação entre o número de pixels com um níveis de cinza pertence ao intervalo (150, 253) e o número de pixels com nível de cinza que pertence ao intervalo (1, 149);

- **Níveis de Cinza 2**: Correspondente à relação entre o número de pixels com um nível de cinza que pertence ao intervalo (246, 256) e o número de pixels com um nível de cinza que pertence ao intervalo (1, 245).

Para avaliar o desempenho de classificação, foram adotados os seguintes parâmetros, utilizados durante a competição LivDet 2009 (Marcialis et al., 2009):

- **Ferrlive**: taxa de impressões digitais de dedo com vida classificadas incorretamente.

- **Ferrfake**: taxa de impressões digitais falsas classificadas incorretamente.

Por fim, o indicador do desempenho é determinado a partir da média:

$$e = \frac{Ferrlive + Ferrfake}{2}$$

Na Tabela 3.3 são apresentados os resultados do método baseado em estatísticas de primeira ordem proposto por Marasco & Sansone (2010) utilizando a base de dados LivDet 2009.

Tabela 3.3: Desempenho do método baseado em histograma proposto por Marasco & Sansone (2010) utilizando a base de dados LivDet 2009. Adaptado de (Marasco & Sansone, 2010).

	Biometrika	**CrossMatch**	**Identix**	**Média**
Ferrlive	12.2%	17.4%	8.3%	12.6%
Ferrfake	13.0%	12.9%	11.0%	12.3%
Média	12.6%	15.2%	9.7%	

3.4 Considerações Finais

Neste capítulo foram apresentadas técnicas para detecção de impressões digitais falsas utilizando características extraídas a partir das imagens das impressões digitais. Inicialmente foi apresentada uma visão geral dos métodos que podem ser utilizados. Na sequência foi descrito um método que utiliza o padrão de transpiração. Em seguida foi apresentado um segundo método que utiliza as estatísticas das quantidades de poros para detecção de vida em impressões digitais. Por fim, foram apresentados métodos que utilizam estatísticas de primeira ordem extraídas de histogramas gerados a partir de imagens de impressões digitais.

Capítulo 4

Material e Métodos

Neste capítulo são apresentados os materiais utilizados nos experimentos e o novo método proposto para realizar a detecção de impressões digitais provenientes de dedos falsos considerando fatores como: resolução das imagens, características de terceiro nível, pressão exercida contra o sensor, tempo de aquisição e umidade do dedo. Por fim é apresentada a metodologia para realização desta dissertação.

4.1 Material

Apesar de existirem bases de dados públicas desenvolvidas com a finalidade de testar o desempenho dos algoritmos de detecção de impressões digitais falsas, estas bases de dados públicas não atendem os requisitos para o desenvolvimento do trabalho proposto nesta dissertação de mestrado, uma vez que as imagens contidas nestas bases de dados contêm no máximo 569dpi.

Alguns experimentos foram realizados para checar se seria possível realizar uma boa detecção de poros nas imagens da base de dados LivDet 2013. Para tanto, o algoritmo proposto por Zhao et al. (2010a) foi utilizado. A Figura 4.1 apresenta o resultado da detecção de poros em algumas imagens. Como pode ser observado o resultado não foi bom.

Devido a baixa resolução das imagens das impressões digitais das bases de dados públicas foi necessária a criação de uma nova base de dados que contém imagens de impressões digitais com alta resolução como descrito na Subseção 4.1.1.

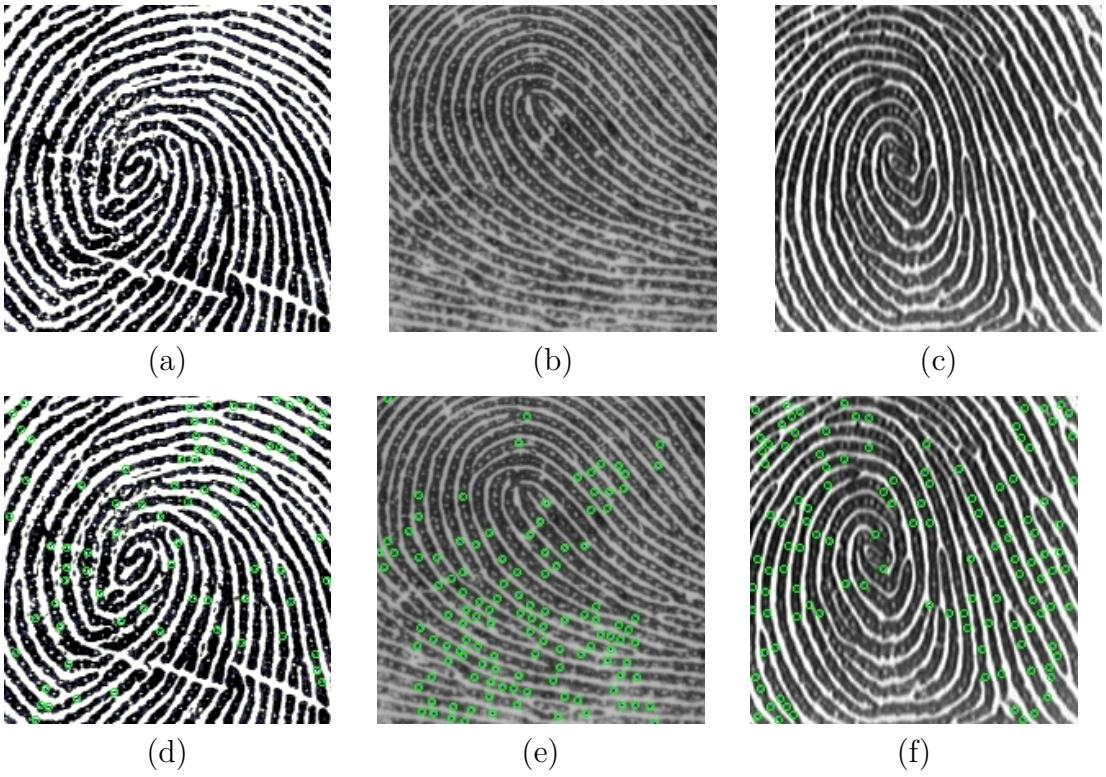


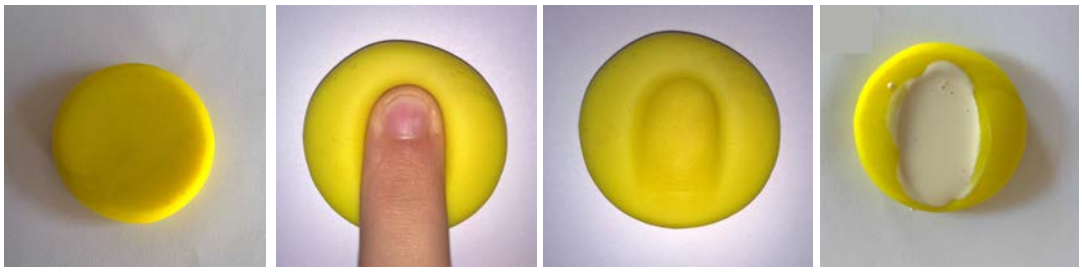
Figura 4.1: Exemplos da performance do algoritmo de detecção de poros proposto por Zhao et al. (2010a) na base de dados LivDet 2013 (Ghiani et al., 2013). (a)-(c) Imagens de impressões digitais capturadas por sensores da CrossMatch, Biometrika e Italdata, respectivamente. (d)-(f) Poros detectados nas imagens de impressões digitais, representados pelos círculos verdes.

4.1.1 Base de Dados UNESP-FSDB

Com o objetivo de analisar o desempenho dos métodos de detecção de impressões digitais falsas utilizando-se informações dos poros sudoríparos e imagens de impressões digitais com diferentes resoluções, diferentes níveis de pressão e diferentes níveis de umidade foi construída uma base de dados própria denominada UNESP *Fingerprint Spoof Database* (UNESP-FSDB). Esta base de dados foi criada por meio da confecção de dedos sintéticos no modo cooperativo utilizando para moldar os dedos massa de modelar SOFT da marca ACRILEX, juntamente com silicone e látex da marca DU LÁTEX (Figura 4.2) para gerar o dedo sintético a partir do molde. Para cada pessoa foram confeccionados oito moldes, sendo quatro do polegar (2 silicone e 2 látex) e quatro do indicador (2 silicone e 2 látex). Na Figura 4.3 são apresentados os passos do processo de fabricação que foram utilizados para geração dos dedos sintéticos.

(a) (b) (c)

Figura 4.2: Materiais utilizados para criação da base de dados UNESP-FSDB. (a) Massa de modelar SOFT da marca ACRILEX, (b) Látex da marca DU LÁTEX e (c) Borracha de Silicone B1 Bege da marca DU LÁTEX.



(a) (b) (c) (d)

Figura 4.3: Processo de fabricação dos dedos sintéticos para captura das imagens da base de dados UNESP-FSDB. (a) Massa de modelar, (b) Voluntário posicionando dedo sobre massa de modelar, (c) Impressão digital moldada na massa de modelar, (d) Massa de modelar preenchida com látex para criação do dedo sintético.

Para checar a qualidade das réplicas foi realizado o cadastramento dos voluntários e suas impressões digitais utilizando-se um software desenvolvido neste trabalho que utiliza o sensor Digital Persona U.are.U 4000B[1] de 512dpi (Figura 4.4(a)). Para cada voluntário, dos 8 dedos confeccionados, apenas 4 (látex e silicone para os dedos indicador e polegar) foram utilizados para criar a base de dados, usando como critério a réplica de melhor qualidade para cada dedo e material, além da pontuação obtida no software desenvolvido. Na Figura 4.4 são apresentados os passos para validação dos dedos sintéticos que foram utilizados na base de dados.

A base de dados UNESP-FSDB contém 6.400 imagens extraídas de 20 voluntários e seus respectivos moldes sintéticos confeccionados de silicone e látex (quatro amostras, sendo duas de silicone e duas látex para os dedos indicador e polegar), utilizando

[1]http://www.smartsec.com.br/digital_persona_u_are_leitor_biometria.html

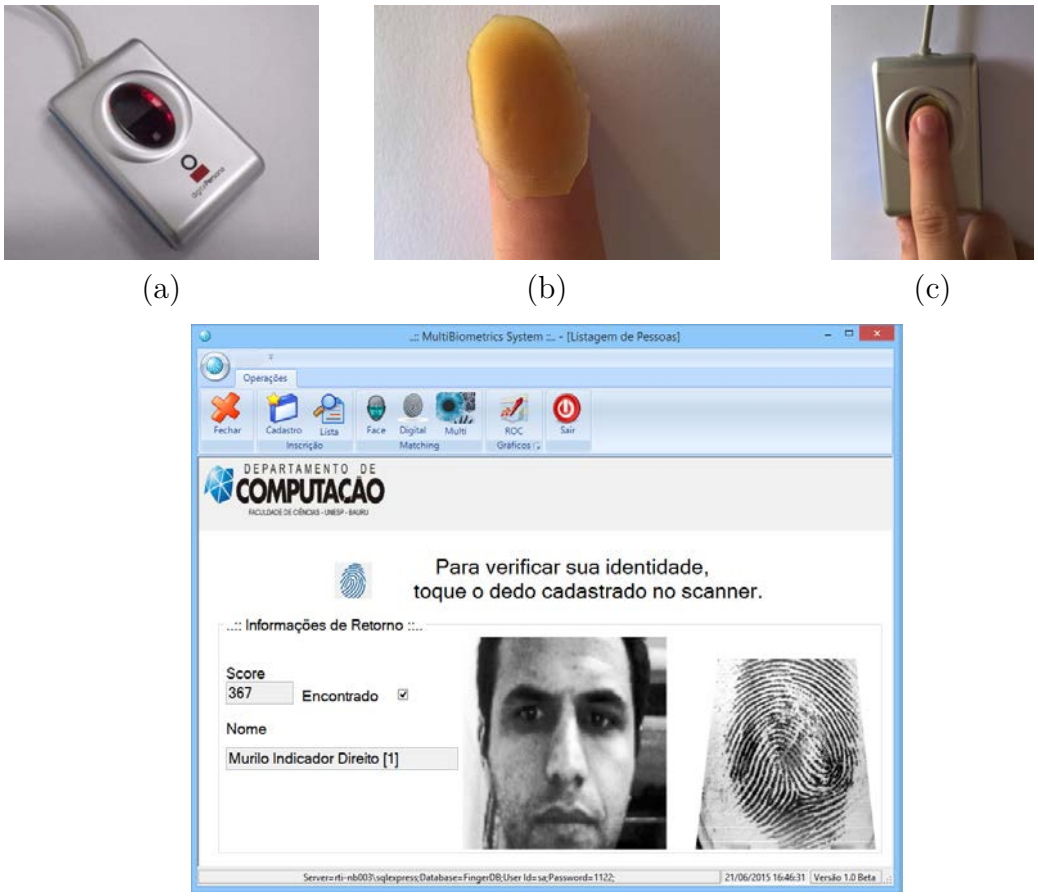


Figura 4.4: Validação da qualidade dos dedos sintéticos. (a) Sensor comercial Digital Persona U Are U 4000b, (b) Dedo sintético, (c) Apresentação do dedo artificial ao sensor e (d) Captura da tela do software desenvolvido onde um impostor conseguiu burlar o sistema com a utilização de um dedo sintético.

o sensor comercial CrossMatch LSCAN 1000T[2] , que permite capturar impressões digitais com 500dpi ou 1000dpi de resolução (Figura 4.5 apresenta uma foto do sensor). A partir dos *spoofs* confeccionados e dos dedos dos voluntários a base de dados foi construída com as seguintes características:

- **Amostras de dedos com vida:** 3.200 impressões digitais, com imagens capturadas de dois dedos diferentes (polegar e indicador), e para cada dedo, duas resoluções diferentes (500dpi e 1000dpi). Para cada resolução, foi solicitado ao voluntário para colocar o dedo sobre a superfície do sensor e 10 impressões digitais foram capturadas sequencialmente com o intervalo de 1 segundo (0 a 9

[2]http://www.crossmatch.com/l-scan-1000px/

segundos). Também foi solicitado ao voluntário para realizar este processo duas vezes para cada resolução, uma pressionando o dedo como de costume (pressão normal) e outra aumentando a pressão (alta pressão). Todo este processo foi repetido duas vezes, na primeira vez os voluntários foram orientados a secar os dedos utilizando uma toalha de papel (subconjunto *DRY*) e na segunda posicionou o dedo no sensor após umedecê-lo em um lenço (subconjunto *WET*).

- **Amostras de dedos falsos:** 3.200 impressões digitais, com imagens capturadas de quatro dedos sintéticos (látex e silicone para o polegar e o indicador). Para cada material e para cada resolução (500dpi e 1000dpi), 10 impressões digitais foram capturadas para cada segundo (0 a 9 segundos). Novamente o processo foi repetido duas vezes para cada resolução, variando a pressão do dedo sobre a superfície do sensor entre normal e alta pressão.

Figura 4.5: Sensor comercial CrossMatch LSCAN 1000T.

Para facilitar a captura das imagens das impressões digitais utilizando o sensor CrossMatch LSCAN 1000T um software foi desenvolvido, a Figura 4.6 apresenta uma tela do software em operação.

A Figura 4.7 mostra alguns exemplos de impressões digitais e moldes da base de dados UNESP-FSDB.

4.1.2 Hardware e Software

Para realização desta dissertação um conjunto de *Hardwares* e *Softwares* foi utilizado para implementação, construção da base de dados e execução dos experimentos:

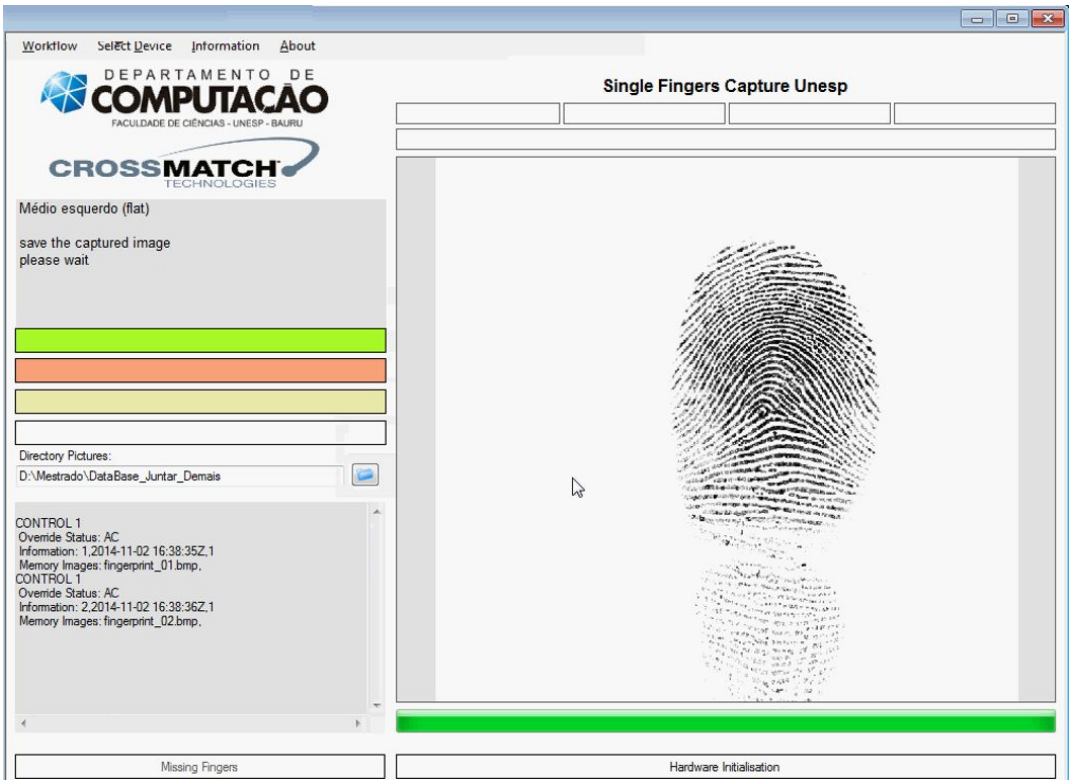


Figura 4.6: Software desenvolvido para captura de impressões digitais utilizando o sensor Cross Match LSCAN 1000T.

- Computador Pessoal (PC): Sistema operacional Windows 7 Ultimate de 64 bits, processador Intel Core i7 de 2.93 GHz, memória RAM de 8GB, HD de 1 TB e placa de vídeo AMD Radeon 2GB DDR5.

- Sensor Digital Persona U Are U 4000B: *scanner* de impressões digitais de único dedo, resolução das imagens 512 dpi, área de captura 14.6 mm x 18.1 mm, dimensões 79 mm x 49 mm x 19 mm, interface de comunicação USB 1.0, 1.1 e 2.0 (Full Speed).

- Sensor CrossMatch LSCAN 1000T: *scanner* de impressões digitais, modos de operação: único dedo, quatro dedos e dois polegares. Resolução das imagens 500 ou 1000 dpi, área de captura 81 mm x 76 mm, temperatura de operação $10 - 35^oC$, dimensões 299 mm x 255 mm x 141 mm, peso 6.9 kg, interface de comunicação IEEE 1394 (FireWire) OHCI interface.

- Visual Studio 2013 Professional Update 3: *Integrated Development Environment* (IDE) utilizado para desenvolvimento do software de captura das impressões

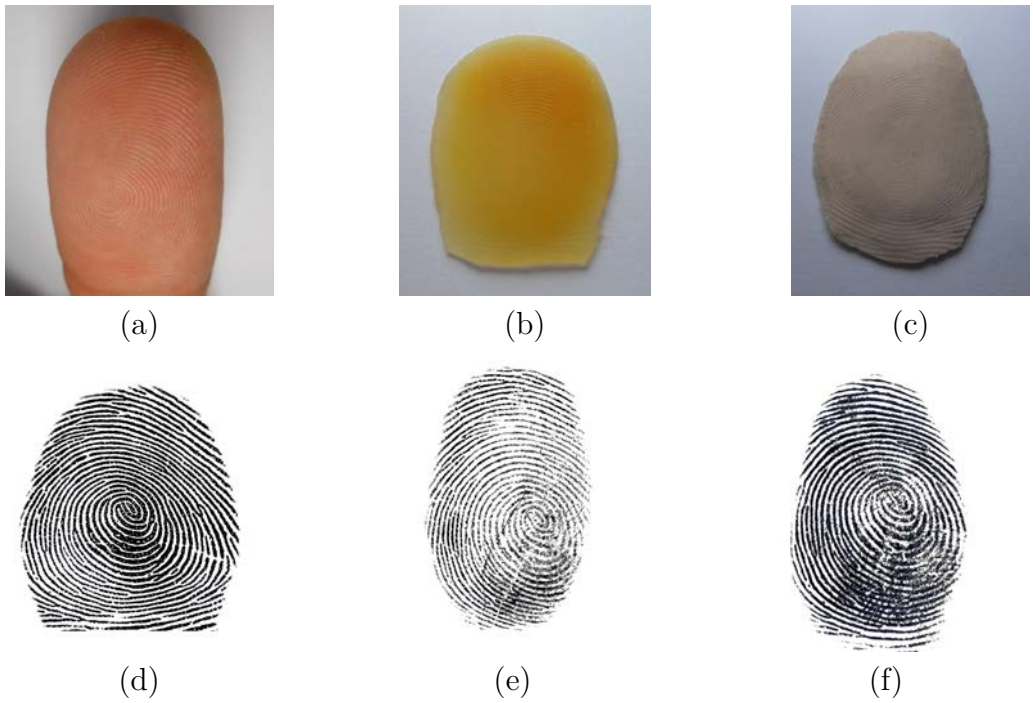


Figura 4.7: Amostras da base de dados UNESP-FSDB. (a) Dedo verdadeiro, (b) Dedo falso confeccionado com látex, (c) Dedo falso confeccionado com silicone, (d) Impressão digital verdadeira, (e) Impressão digital do dedo de látex e (f) Impressão digital do dedo de silicone.

digitais utilizando o sensor CrossMatch LSCAN 1000T e software de cadastramento dos voluntários utilizando o sensor Digital Persona U.are.U 4000B;

- LScan Master SDK: *Software Development Kit* (SDK) desenvolvido pela empresa CROSSMATCH utilizado no software de captura de impressões digitais utilizando o sensor CrossMatch LSCAN 1000T;
- MATLAB R2013a (8.1.0.604) 64-bits: software utilizado para a realização de todos os experimentos e implementação do método de extração de poros proposto por Zhao et al. (2010a);
- Eclipse IDE for Java Developers (Luna Service Release 1 (4.4.1)): software utilizado para implementação do método de extração de poros utilizando filtros isotrópicos descrito por Chaberski (2008) a partir da Toolkit Java.
- *Waikato Environment for Knowledge Analysis* (WEKA) 3.7.11: software utilizado para realizar as classificações utilizando os seguintes classificadores: SVM, KNN, OPF e MLP.

4.2 Método Proposto para Detecção de Dedos Falsos

Neste trabalho, propõe-se o desenvolvimento de um novo método para detecção de *spoofings* em sistemas baseados em impressões digitais. Assim, para cada impressão digital este método deverá classificar a impressão digital como verdadeira ou falsa.

O diagrama do método proposto é apresentado na Figura 4.8 e envolve as seguintes etapas:

1. A imagem da impressão digital, capturada pelo sensor é utilizada como imagem de entrada do método;

2. A partir da imagem de entrada, é criado um vetor de características contendo informações sobre estatísticas de primeira ordem, sobre a qualidade da imagem, sobre a quantidade e a frequência dos poros;

3. O vetor de características é apresentado a um classificador que decide se a impressão digital de entrada é proveniente de um dedo verdadeiro ou de um dedo falso;

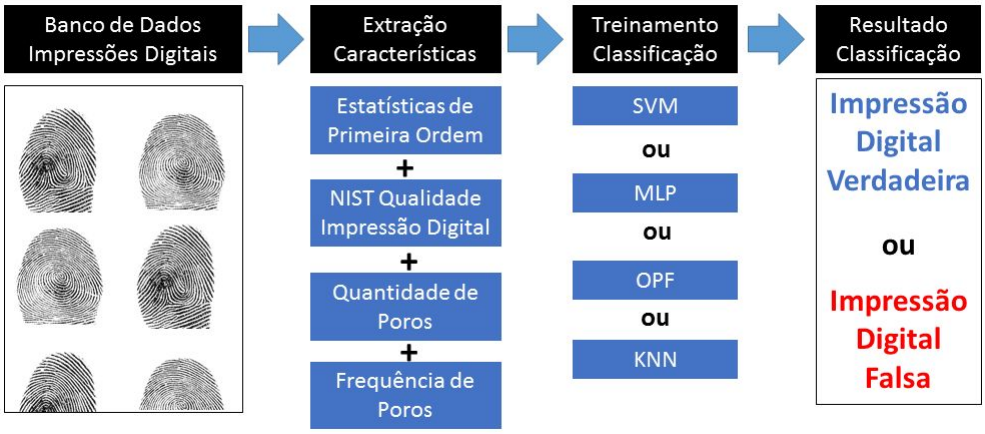


Figura 4.8: Diagrama do novo método proposto para detectar impressões digitais provenientes de dedos falsos.

4.2.1 Extração de Características

As características utilizadas neste trabalho para a detecção de impressões digitais provenientes de dedos verdadeiros ou falsos estão baseadas estatísticas de primeira

ordem dos tons de cinza, qualidade da impressão digital e informação de poros. Para cada impressão digital um vetor de características de nove características é gerado, $F = (F_1, F_2, \ldots, F_9)$. As características extraídas são:

- Estatísticas de primeira ordem: estas características representam as diferenças nos tons de cinza que podem ser observadas entre impressões digitas verdadeiras e falsas, conforme proposto por Abhyankar & Schuckers (2006).

$$F_1 = \sum_{n=0}^{N-1} H(n)^2 \quad \text{(Energia)} \tag{4.1}$$

$$F_2 = \sum_{n=0}^{N-1} H(n) \times logH(n) \quad \text{(Entropia)} \tag{4.2}$$

$$F_3 = \frac{\sum_{n=1}^{N-1} H(n)}{N} \quad \text{(Média)} \tag{4.3}$$

$$F_4 = \sum_{n=0}^{N-1} (n-\mu)^2 H(n) \quad \text{(Variância)} \tag{4.4}$$

$$F_5 = \frac{1}{\sigma^3} \sum_{n=0}^{N-1} (n-\mu)^3 H(n) \quad \text{(Curtose)} \tag{4.5}$$

$$F_6 = \frac{1}{\sigma^4} \sum_{n=0}^{N-1} (n-\mu)^4 H(n) \quad \text{(Assimetria)} \tag{4.6}$$

  onde $H(n)$ é o histograma dos tons de cinza da impressão digital normalizado e equalizado, N é o número de tons de cinza, μ é a média e σ é o desvio padrão.

- NIST *Fingerprint Image Quality Measure* (NFIQ): esta característica, proposta pelo *National Institute of Standards and Technology* (NIST) em Tabassi et al. (2004), mede a qualidade da impressão digital, a qual é baseada nos mapas de qualidade da imagem e no número e qualidade das minúcias da impressão digital. NFIQ é um valor inteiro entre 1 e 5, onde 1 representa a mais alta qualidade de uma impressão digital e 5 a mais baixa qualidade.

$$F_7 = \text{NFIQ}, \tag{4.7}$$

  onde NFIQ $\in \{1, 2, 3, 4, 5\}$.

- Número de poros: esta característica mede o número total de poros na impressão digital. Para extrair os poros de uma imagem de impressão digital neste trabalho são utilizadas duas técnicas, sendo a primeira utilizando a abordagem adaptativa proposta em Zhao et al. (2010a) (abordagem adaptativa que regula a detecção de acordo com a direção e período das cristas locais e detecta poros em impressões digitais com várias resoluções) e a técnica que utiliza filtros isotrópicos (conforme a implementação disponível na biblioteca de domínio

público L3TK, desenvolvida pelo International Biometric Group (2008b) utilizando a linguagem JAVA).

$$F_8 = \text{Número de poros.} \tag{4.8}$$

- Frequência de poros: esta característica é obtida por meio da análise da intensidade dos tons de cinza ao longo das cristas (Derakhshani et al., 2003). Uma imagem com as cristas afinadas da impressão digital é extraída e utilizada como uma máscara para obter as intensidades dos pixels ao longo das cristas. Maiores detalhes sobre esta medida podem ser encontrados na Seção 3.1 (Derakhshani et al., 2003) .

$$F_9 = \sum_{k=11}^{33} f(k)^2, \tag{4.9}$$

onde $f(k) = \frac{\sum_{i=1}^{n} \left| \sum_{p=1}^{255} S_{1i}^{a}(p) e^{-j2\pi(k-1)(p-1)/256} \right|}{n}$, $S_{1i}^{a} = S_{1i} - média(S_{1i})$, n é o número total de cristas e S_{1i} são os sinais individuais de que representam os tons de cinza ao longo das cristas.

4.2.2 Classificação

Nesta etapa do método proposto, um classificador é utilizado para decidir, a partir do vetor de características a ele apresentado, se a impressão digital é proveniente de um dedo verdadeiro ou de um dedo falso. Como há diversos classificadores propostos na literatura, neste trabalho foram avaliados os seguintes classificadores disponibilizados na plataforma WEKA (Hall et al., 2009): ***Optimum-Path Forest* (OPF)** (Papa et al., 2009), ***Support Vector Machine* (SVM)** (Keerthi et al., 2001), ***Multilayer Perceptron* (MLP)** (Rosenblatt, 1958) e ***k-Nearest Neighbors* (KNN)** (Aha & Kibler, 1991). Os parâmetros dos classificadores foram ajustados de acordo com o estudo apresentado por Amancio et al. (2014). Na Tabela A.1 do Apêndice A são apresentados os parâmetros dos classificadores utilizados nos experimentos.

4.3 Metodologia

Para a realização dos experimentos e avaliação dos resultados do método proposto para detecção de impressões digitais provenientes de dedos falsos foram utilizados dois protocolos de testes, quatro medidas de desempenho e sete cenários de testes que são apresentados nas próximas subseções.

4.3.1 Protocolo de Testes

Para avaliação dos resultados obtidos com o método proposto foram utilizados dois protocolos de teste:

- **Treinamento / Teste**: Neste protocolo, a base de dados original é dividida aleatoriamente em 2 subconjuntos distintos. Após a separação, um subconjunto é utilizado para treinamento do classificador e outro utilizado para teste, este protocolo é o mesmo utilizado na competição LivDet.
- **10-Fold Cross-Validation**: Neste protocolo, a base de dados original é dividida aleatoriamente em 10 subconjuntos distintos. Após a separação um subconjunto é escolhido para ser o conjunto de teste e os 9 subconjuntos restantes são utilizados para treinamento do classificador. Este processo é repetido 10 vezes e cada subconjunto é testado apenas uma vez. A acurácia na etapa de classificação é medida por meio da média aritmética entre todas as 10 classificações. Com a realização de 10 repetições o protocolo garante que toda a base de dados foi testada, assim, espera-se que a variabilidade dos acertos entre as repetições seja a menor possível.

4.3.2 Medidas de Desempenho

Para medir o desempenho do método proposto, foram utilizadas neste trabalho as medidas definidas na competição LivDet 2013 organizada por Ghiani et al. (2013):

- **Ferrlive**: Taxa de impressões digitais provenientes de dedos com vida classificadas incorretamente. Esta medida pode ser entendida como FRR (*False Rejection Rate*).
- **Ferrfake**: Taxa de impressões digitais provenientes de dedos falsos classificadas incorretamente. Esta medida pode ser entendida como FAR (*False Acceptance Rate*).

- **Erro Médio**: Taxa média de erro entre Ferrlive e Ferrfake ponderada pelo número de amostras provenientes de dedos verdadeiros e falsos, respectivamente.
- **Acurácia**: Taxa de impressões digitais classificadas corretamente.

4.3.3 Cenários dos Experimentos Realizados

Para avaliar o desempenho do método proposto para detecção de impressões digitais falsas, foram criados alguns cenários:

- **Detecção de Poros**: Neste cenário de testes os métodos de detecção de poros isotrópico e adaptativo foram avaliados na base de dados UNESP-FSDB, uma comparação entre os métodos foi realizada utilizando imagens de 500 e 1000dpi.
- **UNESP-FSDB Resolução da Imagem**: Neste cenário de testes o método proposto para detecção de impressões digitais falsas foi avaliado na base de dados UNESP-FSDB, uma avaliação dos resultados entre as imagens de 500 e 1000 dpi foi realizada, utilizando o protocolo 10-Fold Cross-Validation.
- **UNESP-FSDB Características de Terceiro Nível - Poros**: Neste cenário de testes o método proposto para detecção de impressões digitais falsas foi avaliado na base de dados UNESP-FSDB. Foi realizada uma avaliação da performance do método proposto quando o número e a frequência de poros foram incluídos na vetor de características, utilizando o protocolo 10-Fold Cross-Validation.
- **UNESP-FSDB Pressão do Dedo Sobre o Sensor**: Neste cenário de testes o método proposto para detecção de impressões digitais falsas foi avaliado na base de dados UNESP-FSDB. Foi realizada uma avaliação da performance do método proposto para imagens capturadas com pressão normal e para imagens com pressão alta, utilizando o protocolo 10-Fold Cross-Validation.
- **UNESP-FSDB Tempo de Aquisição das Imagens**: Neste cenário de testes o método proposto para detecção de impressões digitais falsas foi avaliado na base de dados UNESP-FSDB. Foi realizada uma avaliação da performance do método para as imagens capturadas em 10 segundos e a importância do tempo de permanência do dedo sobre a superfície do sensor, utilizando o protocolo 10-Fold Cross-Validation.

- **UNESP-FSDB Umidade do Dedos**: Neste cenário de testes o método proposto para detecção de impressões digitais falsas foi avaliado na base de dados UNESP-FSDB. Foi realizada uma avaliação da performance do método para as imagens capturadas a partir de dedos umedecidos e dedos secos, utilizando o protocolo 10-Fold Cross-Validation.

4.4 Considerações finais

Este capítulo descreveu o material utilizado nesta dissertação de mestrado, o método proposto para a detecção de impressões digitais provenientes de dedos falsos e a metodologia utilizada. Primeiramente foi apresentada a base de dados utilizada nas avaliações dos métodos e a justificativa para a construção da mesma. Após, foram descritos os *hardwares* e os *softwares* adotados para desenvolvimento do método e execução dos experimentos. Depois, o método proposto foi detalhado, trazendo informações sobre as características utilizadas e dos parâmetros adotados nos classificadores. Por fim, foi apresentada a metodologia utilizada, o protocolo de testes, as medidas de avaliação adotadas neste trabalho e os cenários de testes.

Capítulo 5

Resultados Experimentais

Neste capítulo são apresentados e analisados os resultados experimentais obtidos com o novo método proposto para a detecção de impressões digitais provenientes de dedos falsos. Devido a quantidade de classificadores, protocolos e base de dados utilizados nos experimentos, neste capítulo são apresentados e discutidos apenas os resultados mais relevantes. No Apêndice B estão apresentados todos os resultados obtidos nos experimentos.

5.1 Detecção de Poros

Para avaliar o desempenho dos métodos de extração de poros utilizados neste trabalho, o método isotrópico proposto por Jain et al. (2006) e o método adaptativo proposto por Zhao et al. (2010a), descritos nas Seções 5.1.1 e 5.1.2 foi realizada a marcação manual dos poros de 80 imagens de impressões digitais verdadeiras da base de dados UNESP-FSDB descrita na Seção 4.1.1, sendo 40 imagens com 500dpi e 40 imagens com 1000dpi. Esta marcação foi realizada por duas pessoas. É importante ressaltar que os dois métodos são sensíveis a seus parâmetros de entrada que foram escolhidos de forma empírica e avaliados sobre o conjunto de imagens utilizadas na marcação manual.

Três métricas foram utilizadas para avaliar a precisão da detecção dos algoritmos. A primeira, chamada de *True Detection Rate* (TDR) (taxa de detecção correta), é definida como a razão entre o número de poros corretamente detectados e o número total de poros presentes na imagem. A segunda, chamada de *False Detection Rate* (FDR) (taxa de detecção falsa) é definida como a razão entre o número de poros incorretamente detectados e o total de poros detectados pelo método (Zhao, 2010).

A terceira métrica adotada, chamada de Acurácia de Detecção Global, do inglês *Overall Detection Accuracy* (ODA), é definida como:

$$ODA = \sqrt{TDR.(1 - FDR)}, \tag{5.1}$$

Uma vez que foram anotados os centros dos poros do conjunto verdade e nos métodos são retornadas as coordenadas do centro de massa dos poros detectados, foi utilizada uma caixa delimitadora de tamanho 6, 8 e 10 pixels para avaliar se o poro foi corretamente detectado. A Subseção 5.1.3 apresenta os resultados obtidos utilizando o conjunto verdade da base de dados UNESP-FSDB.

5.1.1 Detecção de Poros Utilizando Filtros Isotrópicos

Neste trabalho foi avaliado o método de detecção de poros baseado em filtros isotrópicos proposto por Jain et al. (2006) e descrito por Chaberski (2008), tendo sido utilizada a implementação do método disponível no SDK *Level 3 Fingerprint Image Toolkit* (L3TK) desenvolvido em JAVA pelo *International Biometric Group* (IBG). O SDK L3TK é composto por uma série de filtros, algoritmos de segmentação e casamento de poros inspirados no trabalho de Jain et al. (2006), e os relatórios técnicos do estudo podem ser acessados publicamente em (International Biometric Group, 2008a).

O SDK L3TK baseado em filtros isotrópicos utiliza uma série de parâmetros para efetuar o pré-processamento e a detecção dos poros, no Apêndice A são apresentados estes parâmetros. A Tabela A.2 descreve os parâmetros utilizados no pré-processamento e a Tabela A.3 descreve os parâmetros utilizados na detecção de poros.

Os parâmetros de pré-processamento que foram utilizados são os parâmetros padrões definidos na *toolkit*. Por outro lado, dois parâmetros utilizados na etapa de extração de poros foram alterados para otimizar a performance da detecção de poros na base de dados UNESP-FSDB.

Estes parâmetros foram definidos empiricamente, testando inúmeras variações sobre um conjunto amostral de cinco imagens do conjunto verdade da base de dados UNESP-FSDB.

5.1.2 Detecção de Poros Utilizando Filtros Adaptativos

Neste trabalho, foi avaliado o método de extração de poros baseado em filtros adaptativos *Dynamic Anisotropic Pore Model* (DAPM), proposto por (Zhao et al., 2010a), tendo sido utilizada a implementação disponibilizada pelos autores, desenvolvida em MATLAB. Os mapas de cristas das imagens de impressões digitais, bem como as máscaras das regiões de interesse (área da impressão digital segmentada), são previamente calculadas utilizando o método de realce das impressões digitais e fornecidas como parâmetros de entrada para o método DAPM.

O método baseado em filtros adaptativos utiliza onze parâmetros para efetuar a extração de poros, estes parâmetros são utilizados nos filtros DAPM e *Difference of Gaussian* (DoG). A Tabela A.4 do Apêndice A apresenta a descrição e os valores dos parâmetros utilizados. Estes parâmetros foram definidos empiricamente, testando algumas variações sobre um conjunto amostral de quarenta imagens do conjunto verdade da base de dados UNESP-FSDB.

Neste método baseado em filtros adaptativos, a imagem de impressão digital é particionada em blocos e para cada um deles é realizada a detecção de poros de acordo com sua classificação. Os blocos que não contêm nenhuma região válida da impressão digital são descartados. Se o bloco não possui sua orientação de crista bem definida, então é aplicado o extrator de poros baseado em filtros isotrópicos proposto em (Zhao et al., 2010b) que utiliza o filtro DoG, caso contrário é aplicado o filtro adaptativo DAPM. Após os poros serem detectados para cada um dos blocos, é aplicado um pós-processamento, validando o tamanho dos poros extraídos e sua posição espacial nas impressões digitais.

5.1.3 Resultados da Detecção de Poros em Imagens de 500 e 1000 dpi

Na Tabela 5.1 são apresentados os resultados da detecção de poros nas imagens de 1000 dpi que foi realizada considerando as marcações realizadas pelas duas pessoas (Pessoa 1 e Pessoa 2) e pela fusão da marcação realizada por estas duas pessoas (Fusão). Para realizar a fusão das marcações manuais foram considerados apenas os poros presentes nas duas marcações que estavam a uma distância euclideana menor do que 10 pixels.

Os resultados obtidos e apresentados na Tabela 5.1 mostram que o aumento da largura da caixa delimitadora, utilizada para o casamento dos poros detectados

Tabela 5.1: Acurácia da detecção de poros dos métodos avaliados em imagens com 1000dpi.

Conjunto Verdade	**Pessoa 1**		**Pessoa 2**		**Fusão**	
Método	Adaptativo	Isotrópico	Adaptativo	Isotrópico	Adaptativo	Isotrópico
Caixa delimitadora 6 pixels						
TDR (%)	56,54	51,50	65,29	54,45	66,51	55,68
FDR (%)	28,30	47,81	36,66	57,15	39,17	58,45
ODA (%)	62,84	51,05	63,08	47,06	62,36	46,92
Caixa delimitadora 8 pixels						
TDR(%)	57,96	53,31	66,47	55,34	67,74	57,32
FDR (%)	26,81	45,88	35,70	56,35	38,28	57,23
ODA (%)	64,26	52,89	64,11	47,89	63,38	48,30
Caixa delimitadora 10 pixels						
TDR (%)	**58,48**	55,47	67,03	57,26	68,10	59,74
FDR (%)	**26,24**	43,47	35,28	54,76	38,00	55,52
ODA (%)	**64,79**	55,14	64,58	49,58	63,69	50,26

de forma automática com os poros marcados manualmente, que fazem parte dos conjuntos verdade (Pessoa1, Pessoa2 e Fusão), implica no aumento da taxa TDR e diminuição da taxa FDR concomitantemente, melhorando, desta forma, a taxa ODA. A Figura 5.1 apresenta os resultados da detecção de poros utilizando os dois métodos (Isotrópico e Adaptativo) em duas imagens da base de dados UNESP-FSDB. O maior tamanho de caixa delimitadora avaliado foi o de largura com dez pixels, pois como pode ser observado na Figura 5.1, este tamanho se aproxima da largura das cristas das impressões digitais da base de dados UNESP-FSDB, local onde se encontram os poros.

Outro aspecto importante que pode ser observado nos experimentos é a superioridade do método adaptativo que obteve os melhores resultados para as três métricas utilizadas (TDR, FDR e ODA), para todos os conjuntos verdade analisados (Pessoa1, Pessoa2 e Fusão) e também para todos os tamanhos de caixa delimitadora (6, 8 e 10 pixels). Os melhores resultados do método adaptativo foram obtidos com a utilização da caixa delimitadora de 10 pixels no conjunto verdade anotado pela Pessoa1, as taxas foram TDR = 58,48%, FDR = 26,24% e ODA = 64,79% que podem ser observadas em negrito na Tabela 5.1. Observando-se as Figuras 5.1(d) e 5.1(f) é possível constatar visualmente a superioridade do método de detecção de poros que utiliza filtros adaptativos. Nestas impressões digitais foram utilizadas caixas delimitadoras com 10 pixels em torno das coordenadas centrais dos poros anotados manualmente pela Pessoa1.

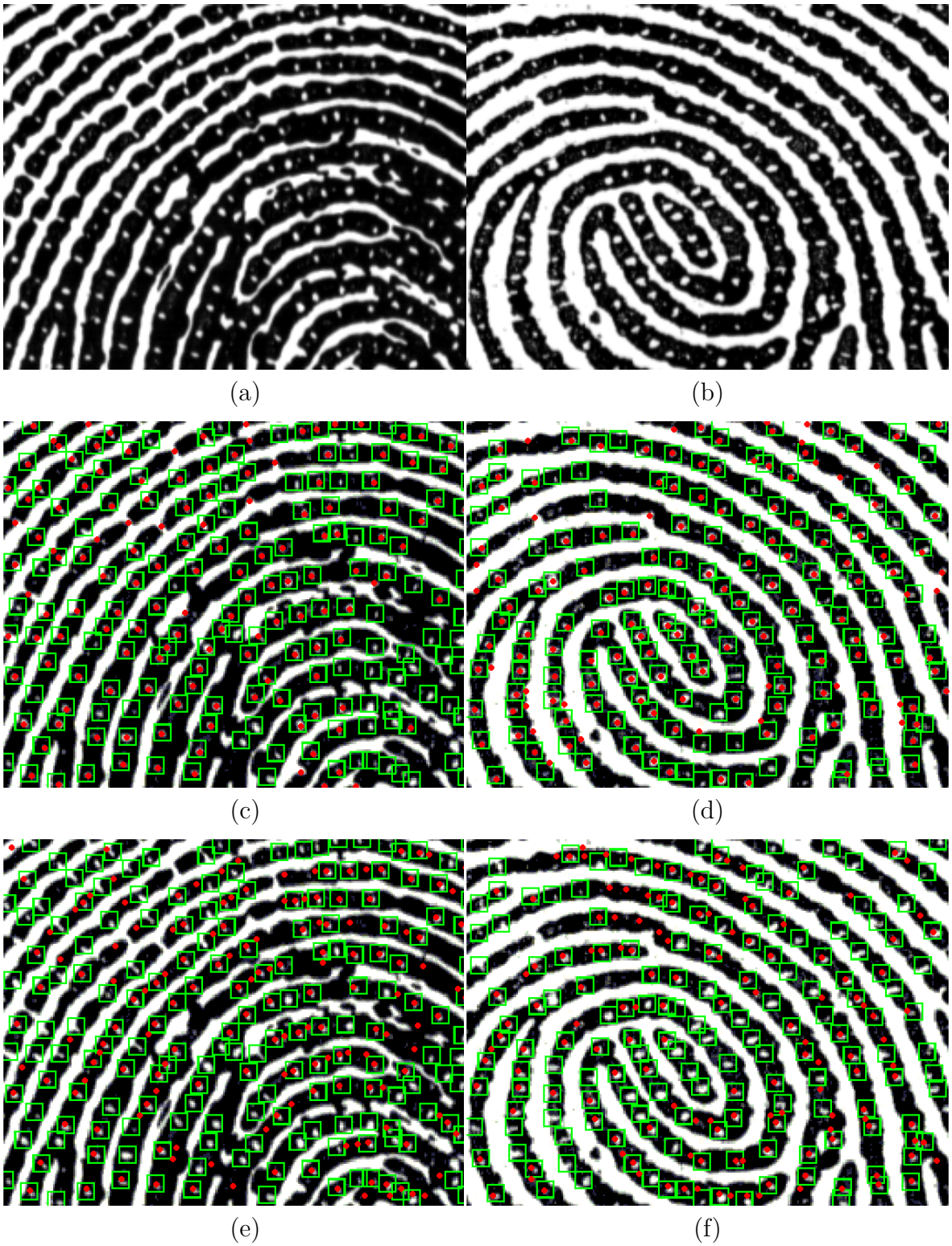


Figura 5.1: Comparativo da detecção de poros dos dois métodos avaliados em duas imagens de 1000 dpi da base de dados UNESP-FSDB.(a)-(b) Imagens originais, (c)-(d) Resultado da detecção de poros utilizando método baseado em filtros adaptativos, e (e)-(f) Resultado da detecção de poros utilizando método baseado em filtros isotrópicos. Os poros detectados estão em destaque na cor vermelha e os poros do conjunto verdade estão denotados pelas caixas delimitadoras 10x10 na cor verde.

Apesar de já existirem trabalhos na literatura relatando que para extração de poros é necessário utilizar imagens com alta resolução ($\geq$ 1000 dpi), como (Jain & Maltoni, 2009) e (Zhao et al., 2008), não foi encontrado na literatura nenhum trabalho relatando o desempenho dos métodos de extração de poros em imagens de 500 dpi. Portanto, neste trabalho foram realizados experimentos utilizando os métodos adaptativo e isotrópico para detecção de poros utilizando imagens com 500 dpi. Nas Tabelas A.3 e A.4 foram apresentados os parâmetros utilizados nos métodos de detecção de poros para imagens com 1000 dpi, no entanto, para obter melhores resultados nas imagens com 500 dpi alguns parâmetros foram modificados sendo eles:

- **(Isotrópico) pe_maximumblobsizeperdpi**: 0.045 (Default);
- **(Isotrópico) pe_mexhatthreshold**: 192 (Default);
- **(Adaptativo) MinPoreSize**: 3 Pixels;

A Tabela 5.2 apresenta os resultados para as imagens de 500 dpi, onde, novamente o aumento da largura da caixa delimitadora ocasiona aumento da performance dos métodos, ou seja, aumento da taxa TDR, diminuição da FDR e consequentemente melhorando a taxa ODA. Para as imagens com 500 dpi, diferentemente do que ocorreu com as imagens com 1000 dpi, o método isotrópico obteve os melhores resultados (Figura 5.2 (d) e (f)), sendo TDR = 52,78%, FDR = 51,20% e ODA = 48,38%, que podem ser observados em negrito na Tabela 5.2, para as marcações da Pessoa1, utilizando uma caixa delimitadora de 6 pixels.

Tabela 5.2: Acurácia da detecção de poros dos métodos avaliados (%) em imagens com 500dpi.

Conjunto Verdade	**Pessoa 1**		**Pessoa 2**		**Fusão**	
Método	Adaptativo	Isotrópico	Adaptativo	Isotrópico	Adaptativo	Isotrópico
Caixa delimitadora 4 pixels						
TDR (%)	19,84	44,66	21,96	43,14	20,27	46,94
FDR (%)	49,93	57,17	41,43	58,90	54,57	60,83
ODA (%)	30,37	41,62	34,43	40,31	29,16	41,03
Caixa delimitadora 6 pixels						
TDR (%)	26,01	**52,78**	24,34	50,93	26,54	54,67
FDR (%)	33,34	**51,20**	35,76	53,34	39,31	55,97
ODA (%)	40,12	**48,35**	37,93	46,72	38,53	46,95

A Figura 5.2 apresenta o resultado da detecção de poros utilizando os dois métodos (Isotrópico e Adaptativo) em duas imagens de 500 dpi na base de dados UNESP-FSDB. Neste caso, o maior tamanho de caixa delimitadora utilizado foi o de seis

pixels de largura, que é a largura máxima de uma crista para as imagens com 500 dpi da base de dados UNESP-FSDB.

Através dos experimentos realizados em imagens com 500 e 1000 dpi foi possível observar que a taxa TDR alcançada no melhor caso para cada resolução foi de 58,48% (1000 dpi/adaptativo) e de 52,78% (500 dpi/isotrópico), já no caso da FDR foram obtidas as taxas de 26,24% (1000 dpi adaptativo) e de 51,20% (500 dpi isotrópico), como a taxa FDR foi muito alta para as imagens de 500 dpi acabou degradando a ODA que foi de 64,79% (1000 dpi adaptativo) e bem menor 48,35% (500 dpi isotrópico), este número alto para FDR indica que o método isotrópico detectou muitos falso-positivos para as imagens com 500 dpi. Embora os resultados indiquem que para detecção de poros as imagens com alta resolução obtêm um melhor desempenho, algumas observações devem ser levadas em consideração:

1. Os métodos utilizados (adaptativo e isotrópico) foram desenvolvidos para serem utilizados em imagens com alta resolução com otimizações para este tipo de imagem, deste modo, naturalmente vão produzir melhores resultados para impressões digitais com 1000 dpi;

2. Os parâmetros foram definidos de forma empírica utilizando um conjunto de 80 imagens (40 com 500 dpi e 40 com 1000 dpi) e podem influenciar nos resultados;

3. Ainda que imagens com 1000 dpi consigam registrar maiores detalhes das impressões digitais como características de terceiro nível, poros também podem ser visualizados em imagens com 500 dpi (Figura 5.2 (a) e (b)).

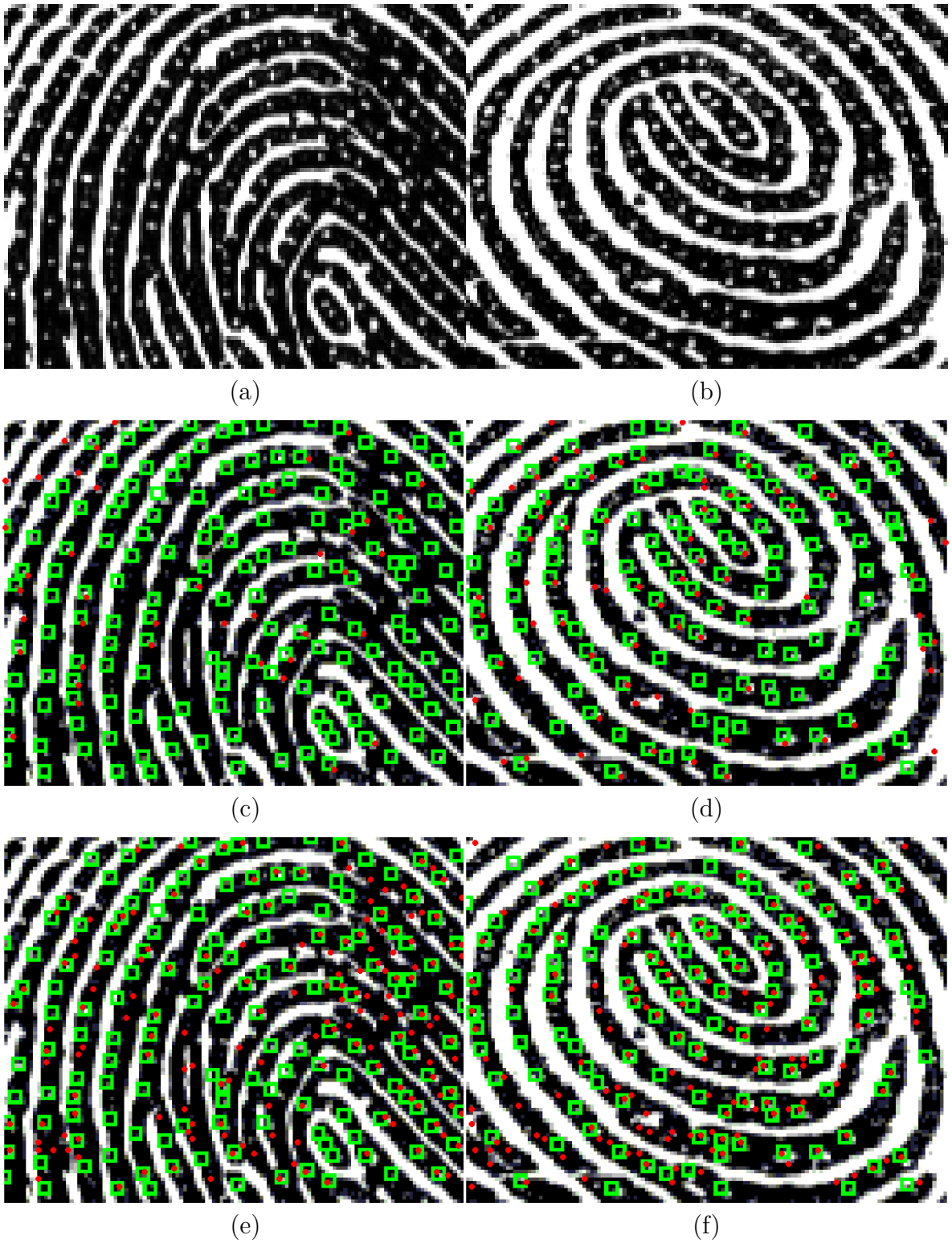


Figura 5.2: Comparativo da detecção de poros dos dois métodos avaliados em duas imagens de 500 dpi da base de dados UNESP-FSDB.(a)-(b) Imagens originais, (c)-(d) Resultado da detecção de poros utilizando método baseado em filtros adaptativos, e (e)-(f) Resultado da detecção de poros utilizando método baseado em filtros isotrópicos. Os poros detectados estão em destaque na cor vermelha e os poros do conjunto verdade estão denotados pelas caixas delimitadoras 6x6 na cor verde.

5.2 Detecção de Impressões Digitais Falsas

Nesta seção são apresentados os resultados obtidos com o novo método utilizando a base de dados UNESP-FSDB, que contém imagens com resolução normal (500 dpi) e alta (1000 dpi), com pressão normal e alta, diferentes tempos de aquisição e imagens capturadas com os dedos secos e umedecidos. Além destes cenários são apresentados resultados de experimentos realizados adicionando informações de poros com o intuito de melhorar a performance da classificação. A fim de facilitar a leitura e discussão dos resultados, apenas os resultados mais relevantes serão apresentados nesta seção, o classificador *Support Vector Machine* (SVM) alcançou os melhores resultados na maioria dos cenários, deste modo os resultados apresentados são dos experimentos realizados utilizando. O classificador SVM com o protocolo 10-Fold Cross-Validation. No Apêndice B estão as Tabelas B.3, B.4, B.5 e B.6 que contêm todos os resultados do experimentos realizados utilizando os classificadores *k-Nearest Neighbors* (KNN), *Multilayer Perceptron* (MLP), *Optimum-Path Forest* (OPF) e SVM e os protocolos de teste relatados na Seção 4.3.1.

5.2.1 Resolução da Imagem

Em geral, acredita-se que imagens de impressão digital com alta resolução automaticamente trazem algum ganho na performance dos algoritmos de classificação de impressões digitais falsas devido à grande quantidade de detalhes que podem ser extraídos das mesmas. Nossos experimentos na base de dados UNESP-FSDB sugerem que esta tendência não se aplica para todas os casos. Na Figura 5.3 é possível visualizar duas impressões digitais da base de dados UNESP-FSDB em 500 e 1000 dpi e uma região em detalhe ampliada onde é possível notar que a imagem de 500 dpi apresenta uma quantidade menor de detalhes da impressão digital.

A acurácia da classificação do método de detecção de impressões falsas proposto neste trabalho alcançou 99,50% para imagens com 500 dpi e um pouco melhor 99,60% quando imagens com 1000 dpi foram utilizadas, isso para a base de dados com imagens *WET*, ou seja, para imagens onde os voluntários utilizaram lenços para umedecer os dedos. Por outro lado, o método alcançou uma taxa de acurácia de 98,60% para imagens com 500 dpi e um pouco pior, 97,80% para 1000 dpi, para a base de dados com imagens *DRY*, imagens onde os voluntários utilizaram um lenço de papel para secar os dedos. Na Tabela 5.3 são apresentadas a acurácia, ferrlive e ferrfake para imagens com 1000 e 500 dpi.

A conclusão que imagens com alta resolução vão degradar a performance comparada com imagens de baixa resolução não pode ser obtida a partir dos experimentos realizados, dado que as imagens não foram capturadas no mesmo momento para as diferentes resoluções, então a variação nos erros pode ser apenas resultado de pequenas mudanças que podem ocorrer durante diferentes processos de captura das imagens (exemplo: área capturada, quantidade de umidade, pressão, etc.), Entretanto, os experimentos podem comprovar que apenas a utilização de imagens de impressões digitais com alta resolução não aumenta automaticamente a performance do método de detecção de impressões digitais falsas, para tanto, é preciso selecionar um conjunto de características que consigam utilizar os detalhes adicionais que podem sem encontrados nas imagens com alta resolução.

Tabela 5.3: Acurácia, Ferrlive e Ferrfake da classificação em (%) do método proposto neste trabalho utilizando imagens de 1000 dpi e 500 dpi.

Base de Dados	**1000 dpi**			**500 dpi**		
	Acurácia(%)	Ferrlive(%)	Ferrfake(%)	Acurácia(%)	Ferrlive(%)	Ferrfake(%)
UNESP-FSDB DRY	97,80	1,10	4,40	98,60	0,50	3,10
UNESP-FSDB WET	99,60	0,30	0,60	99,50	0,30	1,00

5.2.2 Características de Terceiro Nível - Poros

Como descrito na Seção 3.2, outros trabalhos já propuseram o uso de informações sobre os poros para detectar impressões digitais falsas. Espinoza & Champod (2011) utilizaram a diferença na quantidade de poros entre uma imagem de referência e uma imagem distorcida de consulta. Já em Marcialis et al. (2010) foram utilizadas as diferenças no número de poros em certas regiões da impressão digital coletada em 5 segundos (neste período, o usuário tinha que manter o dedo no sensor).

No método proposto neste trabalho é utilizado apenas o número de poros combinado com outras características extraídas da imagem de consulta, assim é necessário apenas uma imagem para decidir se uma impressão digital é verdadeira ou falsa. Com nossos experimentos concluímos que o número de poros detectados em uma impressão digital não é discriminativo o suficiente para determinar se tal impressão digital é proveniente de um dedo verdadeiro ou de um dedo falso, mas, este dado, aliado com a frequência dos poros é uma informação importante para esta tomada de decisão.

A Tabela 5.4 mostra os resultados das classificações das amostras de teste da base de dados UNESP-FSDB: i. quando não é utilizada nenhuma informação sobre

Figura 5.3: Imagens da base de dados UNESP-FSDB. (a) Impressão digital capturada em 1000 dpi, (b) Impressão digital capturada em 500 dpi, (c) detalhe da região central da impressão digital em 150 x 150 pixels em 1000 dpi e (d) detalhe da região central da impressão digital em 75 x 75 pixels em 500 dpi.

poros, ou seja, o vetor de características é composto por apenas (F1-F7), ii. quando a frequência de poros é utilizada, mas não é utilizada a quantidade de poros, ou seja, o vetor de características é composto por (F1-F7 e F9), e iii. quando a quantidade de poros é utilizada juntamente com a frequência de poros, ou seja, o vetor de características é composto por (F1-F9) para imagens com 500 dpi e 1000 dpi. Pode ser observado que a adição das informações de poros (F8 e F9) aumenta a performance do classificador nas duas resoluções, tanto para imagens capturadas a partir de dedos secos (*DRY*) quanto para imagens capturadas a partir de dedos umedecidos (*WET*), chegando a taxas de acurácia de 99,42% (1000 dpi WET) e 99,29% (500 dpi WET).

Tabela 5.4: Acurácia, Ferrlive e Ferrfake da classificação em (%) da combinação de características proposta neste trabalho utilizando informações de poros para imagens de 1000 dpi e 500 dpi.

UNESP FSDB	Características Utilizadas	1000 dpi			500 dpi		
		Acurácia(%)	Ferrlive(%)	Ferrfake(%)	Acurácia(%)	Ferrlive(%)	Ferrfake(%)
WET	F1,F2,F3,F4,F5,F6,F7	98,67	0,60	2,80	98,58	1,30	1,80
	F1,F2,F3,F4,F5,F6,F7,F9	99,13	0,60	1,40	99,17	0,30	1,90
	F1,F2,F3,F4,F5,F6,F7,F8,F9	99,42	0,40	1,00	99,29	0,30	1,60
DRY	F1,F2,F3,F4,F5,F6,F7	89,46	6,80	18,00	88,29	5,60	23,90
	F1,F2,F3,F4,F5,F6,F7,F9	93,21	3,20	14,00	96,58	1,30	7,80
	F1,F2,F3,F4,F5,F6,F7,F8,F9	95,29	2,40	9,30	97,50	0,80	5,90

5.2.3 Pressão do Dedo Sobre o Sensor

Durante a captura das impressões digitais da base de dados UNESP-FSDB foi solicitado aos voluntários para aplicarem um pressão normal do dedo na superfície do sensor na primeira aquisição e para aumentarem a pressão na segunda aquisição. Na Figura 5.4 é possível visualizar as diferenças entre as imagens capturadas com pressão normal e com pressão alta para dedos verdadeiros (DRY) (Figuras 5.4(a) e 5.4(b)), para dedos de látex (Figuras 5.4(c) e 5.4(d)) e para dedos de silicone (Figuras 5.4(e) e 5.4(f)). As impressões digitais dos dedos falsos (Silicone e Látex) apresentam um padrão de deformação diferente de um dedo humano, o silicone como é um material mais macio quando se utiliza uma pressão maior sofre uma deformação que acaba unificando as cristas, formando uma região preta borrada na impressão digital conforme Figura 5.4 (f). Portanto, a utilização de uma pressão maior pode facilitar a tarefa de classificação entre impressões digitais falsas e verdadeiras, particularmente para a detecção das impressões digitais provenientes de dedos de silicone.

Na Tabela 5.5 é possível notar que a performance do método proposto aumentou quando foram utilizadas as imagens das impressões digitais obtidas quando o usuário aplicou maior pressão dos dedos contra o sensor. Na base de dados com imagens capturadas a partir dos dedos que utilizaram um lenço de papel para remover a umidade (DRY) com 500dpi, a acurácia aumentou de 98.33% para 98.42% e para imagens com 1000dpi aumentou de 96.75% para 97.92%. Este aumento na performance está relacionado ao aumento da taxa de acerto nas impressões verdadeiras que foram classificadas como verdadeiras e impressões falsas que foram classificadas como falsas.

Por outro lado, a performance do método teve uma pequena queda no desempenho para a base de dados com imagens capturadas a partir de dedos que utilizaram um lenço umedecido (WET). Para imagens com 500dpi a performance caiu de

99,58% (pressão normal) para 99,42% (pressão alta). Para imagens com 1000 dpi a performance caiu de 99,83% (pressão normal) para 99,75% (pressão alta). Esta pequena queda está relacionada com o aumento das taxas de erro ferrlive e ferrfake. Como os resultados já eram muito bons com as imagens capturadas a partir de dedos umedecidos e pressão normal (99,83% 500dpi e 99,75% 1000dpi) a utilização de pressão acabou degradando levemente o resultado. Porém, para base de dados em condições normais, esta estratégia de emprego de uma pressão maior pode ser utilizada para melhorar as taxas de acerto.

Tabela 5.5: Acurácia, Ferrlive e Ferrfake da classificação em (%) da combinação de características proposta neste trabalho para pressão normal e alta.

UNESP FSDB	**Pressão Aplicada no Sensor**	**1000 dpi**			**500 dpi**		
		Acurácia(%)	Ferrlive(%)	Ferrfake(%)	Acurácia(%)	Ferrlive(%)	Ferrfake(%)
DRY	Alta	97,92	0,60	5,00	98,42	0,60	3,50
	Normal	96,75	1,50	6,80	98,33	0,60	3,80
WET	Alta	99,75	0,30	0,30	99,42	0,40	1,00
	Normal	99,83	0,30	0,10	99,58	0,30	0,80

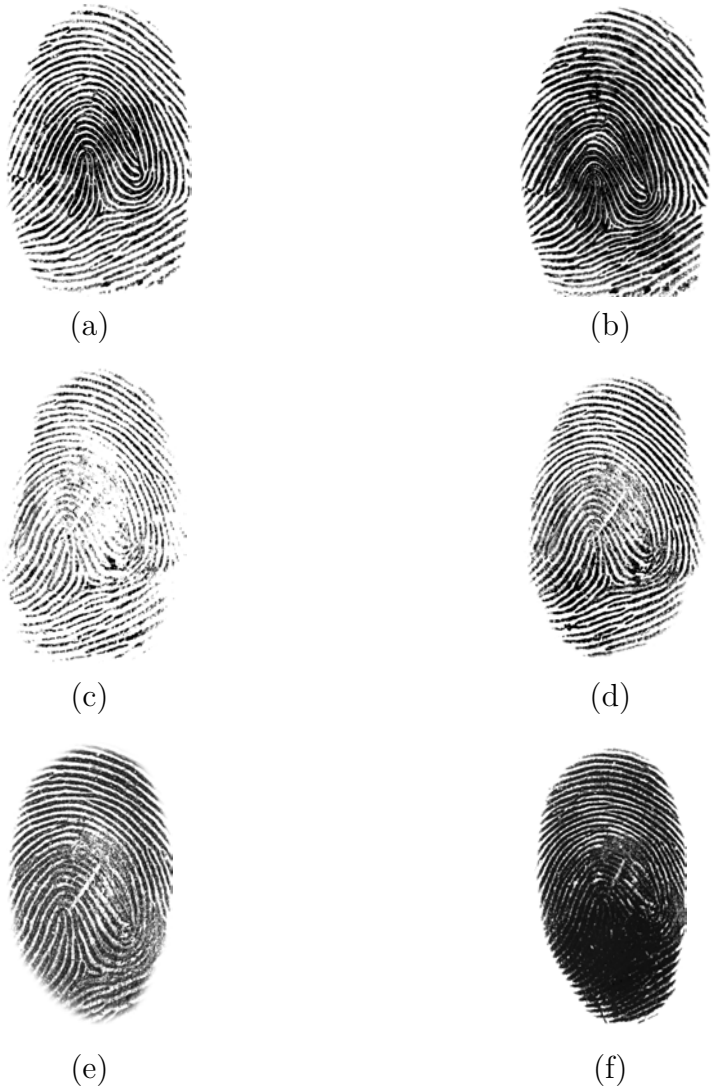


Figura 5.4: Imagens da base de dados UNESP-FSDB em 1000dpi com pressão normal e alta. Dedos verdadeiros - DRY (a) pressão normal e (b) pressão alta, Dedos de Látex (c) pressão normal e (d) pressão alta, Dedos de Silicone (e) pressão normal e (f) pressão alta.

5.2.4 Tempo de Aquisição das Imagens

Na coleta da base de dados UNESP-FSDB foi solicitado aos voluntários que mantivessem o dedo sobre a superfície do sensor por 10 segundos, neste período 10 impressões digitais foram capturadas, uma por segundo. O objetivo de capturar as imagens seguindo este protocolo é avaliar as alterações da qualidade das imagens capturadas no decorrer de 10 segundos e analisar o desempenho do método proposto para as

imagens capturadas a cada segundo. Pode-se analisar que, em geral, a primeira imagem captura é de má qualidade e que a partir da segunda imagem a qualidade da imagem melhora consideravelmente. Para Derakhshani et al. (2003) a diferença entre a primeira imagem e as demais está relacionada ao processo de transpiração, ou seja, no momento da captura da primeira imagem o dedo ainda não iniciou o processo de transpiração e as imagens ficam com uma tonalidade desigual. Acreditamos que a baixa qualidade da primeira imagem pode também estar relacionada à falta de pressão adequada ou mau posicionamento do dedo no inicio da captura (1º segundo). Na Figura 5.5 é possível visualizar as diferenças das tonalidades das impressões digitais capturadas no primeiro e no quinto segundos, respectivamente.

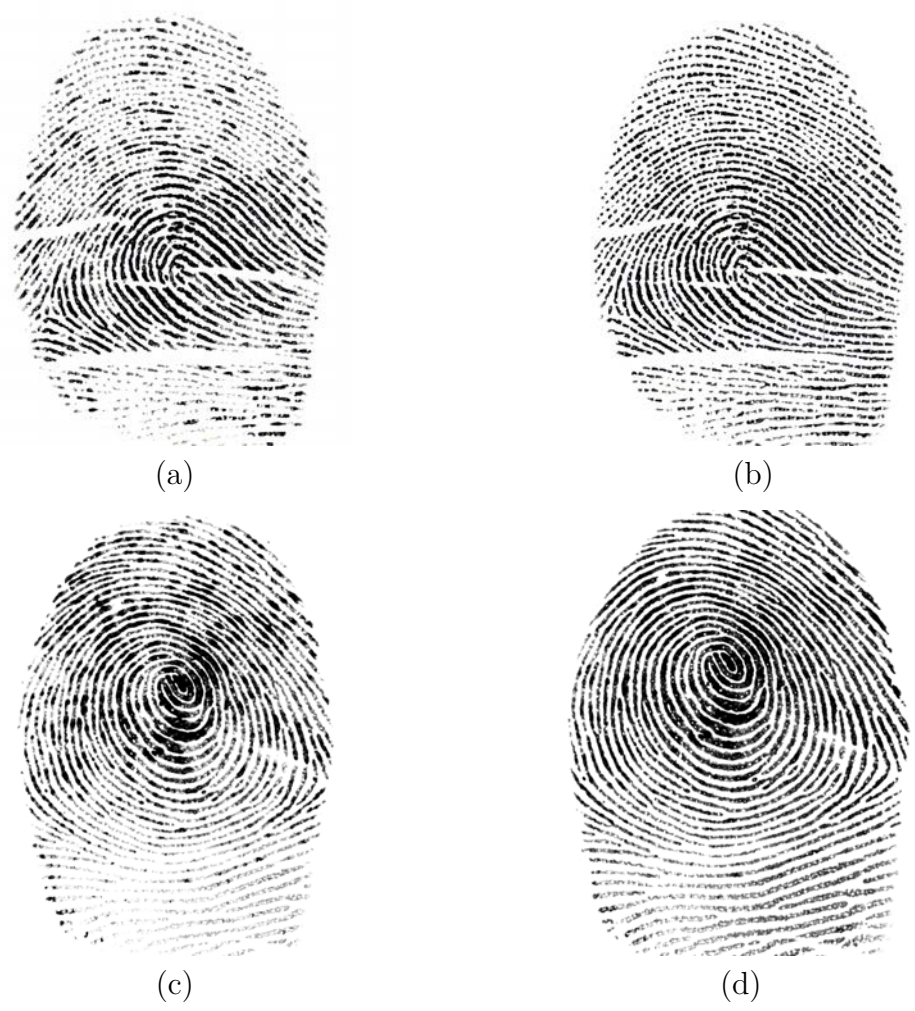


Figura 5.5: Exemplos de imagens da base de dados UNESP-FSDB com 1000 dpi. (a) e (c) Imagem capturada no primeiro segundo e (b) e (d) imagem captura no quinto segundo.

Na Tabela 5.6 são apresentados os resultados obtidos para as imagens capturadas no decorrer dos 10 segundos, as imagens foram separadas em 3 grupos sendo: (1,2,3) grupo com imagens capturadas nos três segundos iniciais, (4,5,6) para imagens capturadas entre o quarto e sexto segundo e (7,8,9,10) para as imagens capturadas nos quatro segundos finais. De uma forma geral os resultados do primeiro grupo (1,2,3) não são bons, sendo 91.81% para imagens com 1000 dpi e 96.11% para imagens com 500 dpi, para a base de dados (DRY). Isso ocorre pois como relatado as imagens do primeiro segundo apresentam má qualidade. Entretanto, para as imagens do segundo grupo (4,5,6) os resultados melhoram sendo 96.25% e 99.44% para imagens com 1000 e 500 dpi respectivamente. O terceiro e último grupo de imagens (7,8,9,10), no geral, não apresenta melhora significativa nos resultados com relação ao grupo anterior, portanto, manter o dedo sobre a superfície do sensor por um tempo maior do que seis segundos não contribui muito para o processo de classificação com o método proposto.

Tabela 5.6: Acurácia, Ferrlive e Ferrfake da classificação em (%) da combinação de características proposta neste trabalho para imagens capturadas no decorrer de 10 segundos

UNESP FSDB	**Tempo de Captura das Imagens**	**1000 dpi**			**500 dpi**		
		Acurácia(%)	Ferrlive(%)	Ferrfake(%)	Acurácia(%)	Ferrlive(%)	Ferrfake(%)
DRY	1,2,3 Seg	91,81	4,80	15,00	96,11	1,70	8,30
	4,5,6 Seg	96,25	3,30	4,60	99,44	0,20	1,30
	7,8,9,10 Seg	98,02	1,10	3,80	99,38	0,50	0,90
WET	1,2,3 Seg	98,61	1,00	2,10	97,36	2,10	3,80
	4,5,6 Seg	99,58	0,20	0,80	99,58	0,20	0,80
	7,8,9,10 Seg	99,69	0,20	0,60	100,00	0,00	0,00

5.2.5 Umidade do Dedo

Jain et al. (2007) relataram que dentre as características de terceiro nível, os contornos das cristas são mais confiáveis do que os poros uma vez que as variações da condição da pele, do clima e dos ruídos do sensor podem interferir na detecção de poros em uma impressão digital. Na Figura 5.6 são apresentadas duas imagens da mesma impressão digital, com quantidades distintas de poros detectados, o que mostra que pode haver grande variabilidade desta informação.

Durante a captura das imagens para confecção da base de dados UNESP-FSDB e realização dos experimentos conforme já relatado por Jain et al. (2007), foi possível constatar que muitas imagens, mesmo com alta resolução (1000 dpi) não apresentavam uma quantidade significativa de poros. Diante disso foi constatado que alguns fatores

Figura 5.6: Duas impressões digitais do mesmo dedo em 1000 dpi. Pode ser observado que das características de 3º nível de impressões digitais os contornos das cristas são mais confiáveis do que os poros (Jain et al., 2007).

podem influenciar para que os poros apareçam ou não em uma impressão digital, sendo eles:

- **Fatores climáticos**: As imagens da base de dados UNESP-FSDB foram capturadas em um período seco do ano, e a baixa umidade relativa do ar influência na qualidade da impressões digitais;
- **Ambiente climatizado**: O local utilizado para capturar as impressões digitais possui sistema de refrigeração que funciona 24 horas, 7 dias por semana, e ambientes refrigerados contribuem para diminuir a umidade relativa do ar;
- **Condição do dedo**: Como uma medida para padronizar a captura, foi solicitado aos voluntários para secar o dedo com um lenço de papel. Este procedimento acabou removendo a umidade natural da pele do dedo e contribuiu para a baixa qualidade das impressões digitais;

- **Superfície do sensor**: Se a superfície do sensor não estiver adequadamente limpa, a qualidade da imagem da impressão digital, bem como a captura dos poros pode ser prejudicada.

A Figura 5.7 apresenta dois fragmentos de impressões digitais do mesmo dedo em 1000 dpi. A Figura 5.7(a) apresenta uma impressão digital capturada a partir de um dedo que foi seco com um lenço de papel e a Figura 5.7(b) apresenta uma impressão digital capturada a partir de um dedo que foi umedecido com um lenço. Pode-se observar que a quantidade de poros detectados na impressão digital capturada do dedo úmido é bem maior do que os poros detectados na impressão digital capturada do dedo seco.

(a) (b)

Figura 5.7: Duas imagens da mesma impressão digital da base de dados UNESP-FSDB, capturadas com 1000 dpi. (a) Dedo seco; (b) Dedo úmido.

Na Tabela 5.7 são apresentados os resultados da performance alcançada pelo método proposto avaliando o impacto da umidade no processo de detecção de impressões falsas, tanto para impressões em 500 dpi quanto em 1000 dpi. Os resultados são melhores para impressões digitais capturadas a partir de dedos umedecidos. Para imagens com 1000 dpi a acurácia saltou de 97,83% (DRY) para 99,58% (WET) e com 500 dpi de 98,63% (DRY) para 99,46% (WET).

Portanto, com os experimentos realizados ficou evidente que os poros, características de terceiro nível, são muito vulneráveis às condições externas e devem ser utilizados com cautela para atividades de reconhecimento e detecção de impressões digitais falsas.

Tabela 5.7: Acurácia, Ferrlive e Ferrfake da classificação em (%) do método proposto para impressões digitais provenientes de dedos secos (DRY) e umedecidos (WET).

Umidade do dedo	**1000 dpi**			**500 dpi**		
	Acurácia(%)	Ferrlive(%)	Ferrfake(%)	Acurácia(%)	Ferrlive(%)	Ferrfake(%)
Seco (DRY)	97,83	1,10	4,40	98,63	0,50	3,10
Úmido (WET)	99,58	0,00	0,60	99,46	0,30	1,00

5.3 Considerações finais

Este capítulo descreveu os experimentos realizados neste trabalho. Primeiramente foram avaliados os algoritmos de detecção de poros isotrópico e adaptativo para imagens de 500 e 1000 dpi. Posteriormente foram realizados experimentos na base de dados UNESP-FSDB e realizado a discussão acerca dos resultados obtidos.

Capítulo 6

Conclusões

Atualmente, a utilização de sistemas biométricos em aplicações comercias e governamentais aumentou significativamente, particularmente os sistemas baseados em impressões digitais. Paralelamente, muitos casos de fraude têm sido constatados recentemente, fato que tem motivado a realização de pesquisas visando desenvolver e aperfeiçoar as técnicas para detecção de ataques aos sistemas biométricos, em particular, os ataques aos sensores, conhecidos como *spoofing*.

As pesquisas para detecção de *spoofing* são relativamente recentes se comparadas às pesquisas na área de Biometria. A primeira competição para comparação de métodos de detecção de *spoofing*, a *Fingerprint Liveness Detection Competition* (LivDet), foi realizada no ano de 2009 e tem se repetido a cada dois anos, enquanto que a primeira competição para comparação de métodos de reconhecimento de impressões digitais, a *Fingerprint Verification Competition* (FVC), foi realizada no ano de 2000.

Neste trabalho foi criada uma nova base de dados, denominada UNESP *Fingerprint Spoof Database* (UNESP-FSDB) que contém 6.400 imagens extraídas de 20 voluntários e seus respectivos moldes sintéticos confeccionados com silicone e látex (quatro amostras, sendo duas de silicone e duas de látex para os dedos indicador e polegar), utilizando o sensor comercial CrossMatch LSCAN 1000T, que permite capturar impressões digitais com 500dpi ou 1000dpi de resolução. Além desta característica, esta nova base de dados contém imagens capturadas com diferentes padrões de umidade, pressão e tempo de coleta.

Com a utilização da base de dados própria UNESP-FSDB foi possível realizar um estudo inédito acerca de alguns fatores que podem influenciar os métodos de detecção de impressões falsas, sendo eles: resolução da imagem, características de terceiro

nível, pressão imposta no momento da captura, tempo de aquisição da impressão digital e umidade do dedo no momento da captura.

Inspirado em métodos do estado-da-arte, foi proposto um novo método para detecção de impressões digitais provenientes de dedos falsos, que combina medidas de estatísticas de primeira ordem dos tons de cinza das imagens das impressões digitais, com medidas de qualidade das imagens e medidas de características de terceiro nível das impressões digitais, tais como, quantidade e frequência dos poros sudoríparos detectados nas imagens.

Em relação à resolução das imagens foi possível constatar que a utilização de imagens de alta resolução não trazem necessariamente melhoras para o método proposto para detecção de impressões digitais falsas dado que para imagens da base de dados UNESP-FSDB - WET o aumento foi de 0,10% para as imagens de 500 e 1000dpi, enquanto que para a base de dados UNESP-FSDB - DRY as imagens com alta resolução tiveram uma acurácia 0,80% pior em relação as imagens com 500dpi. Isto pode ter ocorrido devido ao fato que as imagens com alta resolução fornecem uma gama maior de informações e detalhes da impressão digital. Por outro lado, apresentam uma maior quantidade de ruído e necessitam de métodos que consigam tratar de forma eficiente as características de terceiro nível da impressão digital para aumentar a performance da detecção de impressões digitais falsas.

Em relação ao uso de características de terceiro nível, duas medidas foram empregadas, a frequência e a quantidade de poros encontrada na impressão digital, o uso das informações aumentou em 5,83% a acurácia da detecção de impressões digitais falsas para as imagens com 1000 dpi e para imagens com 500 dpi o aumento foi de 9,21%.

Dois fatores externos ao método de detecção também foram avaliados: a pressão do dedo imposta contra o sensor e a umidade do dedo no momento da captura da impressão digital. Com relação a pressão utilizada, para a base de dados UNESP-FSDB - DRY foram registrados aumentos na acurácia tanto para imagens de 1000 dpi (+1,17%) quanto para 500 dpi (+0,09%). Esta melhora esta relacionada com a dinâmica de deformação dos materiais sintéticos. O silicone, por exemplo, é muito mais macio do que a pele humana e deforma-se mais do que esta, causando maior borramento na imagem da impressão digital. Com relação à umidade do dedo, para imagens com 1000 dpi a performance aumentou 1,75% ao utilizar imagens capturadas a partir de dedos umedecidos. Para imagens com 500 dpi, o aumento foi de 0,83%.

estas melhoras na acurácia estão relacionadas a qualidade da imagem e na quantidade de poros que podem ser melhor detectados em dedos mais úmidos.

Por fim, também foi investigada a influência do tempo de aquisição em que o dedo fica em contato com a superfície do sensor. Durante a coleta das impressões digitais, foi solicitado para os voluntários colocarem o dedo sobre a superfície do sensor e manterem-no o dedo posicionado por 10 segundos. As imagens das impressões digitais coletadas foram separadas em três grupos: de 1 a 3 segundos, de 4 a 6 segundos e de 7 a 10 segundos. De forma geral, o primeiro grupo de imagens que contém as imagens capturadas nos três segundos iniciais apresentou uma performance pior do que os demais, pois, a primeira imagem apresenta, em geral, uma qualidade pior do que as demais imagens capturadas no decorrer de dez segundo, esta queda na performance pode chegar a 4,44%, isso indica que a primeira imagem pode ser descartada como uma forma de aumentar a performance do método proposto.

6.1 Contribuições

Ao final deste trabalho as seguinte contribuições podem ser enumeradas:

1. Construção de uma base de dados com 6.400 imagens de impressões digitais provenientes de dedos verdadeiros e falsos;

2. Desenvolvimento de um novo método para detecção de impressões digitais falsas a partir da combinação de medidas estatísticas de primeira ordem dos tons de cinza das imagens, qualidade das imagens e de características de terceiro nível das impressões digitais;

3. Comparação da performance entre dois métodos de detecção de poros (Isotrópico e Adaptativo) utilizando imagens de 500 e 1000 dpi;

4. Avaliação sobre a importância da utilização de imagens com alta resolução para detecção de impressões digitais falsas;

5. Análise da importância da utilização de poros para detecção de impressões digitais falsas;

6. Análise sobre o impacto que a pressão do dedo utilizada no momento da captura pode ocasionar nos resultados;

7. Análise sobre o impacto da umidade do dedo na detecção de poros e classificação de impressões digitais falsas;

8. Análise sobre o tempo de permanência do dedo sobre o sensor e a relação com a qualidade da imagem e taxas de acurácia para detecção de impressões digitais falsas.

6.2 Trabalhos Publicados

Durante a realização desta dissertação de mestrado, foram publicados os seguintes trabalhos relacionados a detecção de impressões digitais provenientes de dedos falsos:

I. **Silva, M. V.**; Marana, A. N. . Detecção de Ataques aos Sensores de Impressões Digitais Utilizando Características de Terceiro Nível. *In: IV WPPGCC - IV Workshop do Programa de Pós-Graduação em Ciência da Computação da UNESP*, Presidente Prudente - Brasil, 2014.

II. **Silva, M. V.**; Marana, A. N.; Paulino, A. A. . On the Importance of Using High Resolution Images, Third Level Features and Sequence of Images for Fingerprint Spoof Detection. *In: ICASSP 2015 - 40th IEEE International Conference on Acoustics, Speech and Signal Processing*, Brisbane - Austrália, 2015.

III. **Silva, M. V.**; Marana, A. N. . Detecção de Impressões Digitais Falsas no Reconhecimento Biométrico de Pessoas. *In: V WPPGCC - V Workshop do Programa de Pós-Graduação em Ciência da Computação da UNESP*, Bauru - Brasil, 2015.

IV. **Silva, M. V.**; Luiz, J. P.; Angeloni, M. A.; Paulino, A. A.; Marana, A. N. . Comparison Between Isotropic and Adaptative Pore Detection Methods for Fingerprint Recognition. *In: WVC 2015 - XI Workshop de Visão Computacional*, São Carlos - Brasil, 2015.

6.3 Trabalhos Futuros

Como continuidade deste trabalho pretende-se:

1. Aumentar a base de dados com voluntários de faixas etárias mais variadas, inclusão de outros materiais para confecção dos dedos sintéticos e geração de impressões falsas utilizando o modo não cooperativo;

2. Investigar métodos baseados na abordagem dinâmica, ou seja, métodos que utilizam mais de uma imagem para detectar se uma impressão é verdadeira ou falsa;

3. Investigar outras características de terceiro nível que possam ser melhor observadas e detectadas nas imagens de impressões digitais com alta resolução;

4. Aprofundar os estudos acerca da dinâmica dos poros e fatores que podem influenciar a captura dos poros pelos sensores.

Referências Bibliográficas

Abhyankar, A. & Schuckers, S. (2006). Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In *Image Processing, 2006 IEEE International Conference on* (pp. 321–324).

Aha, D. & Kibler, D. (1991). Instance-based learning algorithms. *Machine Learning*, 6, 37–66.

Al-Ajlan, A. (2013). Survey on fingerprint liveness detection. In *Biometrics and Forensics (IWBF), 2013 International Workshop on* (pp. 1–5).

Amancio, D. R., Comin, C. H., Casanova, D., Travieso, G., Bruno, O. M., Rodrigues, F. A., & da Fontoura Costa, L. (2014). A systematic comparison of supervised classifiers. *PLoS One*, 9(4), 1–14.

Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G., & Roli, F. (2012). Security evaluation of biometric authentication systems under real spoofing attacks. *Biometrics, IET*, 1(1), 11–24.

Brasil (2012). Projeto de lei 3558/2012 - dispõe sobre a utilização de sistemas biométricos, a proteção de dados pessoais e dá outras providências.

Cavalcanti, G. D. C., Pereira, L., Pinheiro, H., Silva, J., Silva, A., Pina, T., Carvalho, D., & Ren, T. (2012). A modular architecture based on image quality for fingerprint spoof detection. In *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on* (pp. 258–262).

Chaberski, M. (2008). Level 3 Friction Ridge Research. *Biometric Technology Today*, 16(11-12), 9–12.

Choi, H., Kang, R., Choi, K., & Kim, J. (2007). Aliveness detection of fingerprints using multiple static features. 1(4), 151 – 157.

Coli, P., Marcialis, G., & Roli, F. (2007). Vitality detection from fingerprint images: A critical survey. In S.-W. Lee & S. Li (Eds.), *Advances in Biometrics*, volume 4642 of *Lecture Notes in Computer Science* (pp. 722–731). Springer Berlin Heidelberg.

Derakhshani, R., Schuckers, S. A., Hornak, L. A., & O'Gorman, L. (2003). Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition*, 36(2), 383 – 396. <ce:title>Biometrics</ce:title>.

Espinoza, M. & Champod, C. (2011). Using the number of pores on fingerprint images to detect spoofing attacks. In *Hand-Based Biometrics (ICHB), 2011 International Conference on* (pp. 1–5).

Galbally, J., Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. (2012). A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems*, 28(1), 311 – 321.

Ghiani, L., Marcialis, G., & Roli, F. (2012). Fingerprint liveness detection by local phase quantization. In *Pattern Recognition (ICPR), 2012 21st International Conference on* (pp. 537–540).

Ghiani, L., Yambay, D., Mura, V., Tocco, S., Marcialis, G. L., Roli, F., & Schuckcrs, S. (2013). Livdet 2013 fingerprint liveness detection competition 2013. In *Biometrics (ICB), 2013 International Conference on* (pp. 1–6).

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The weka data mining software: An update. *SIGKDD Explor. Newsl.*, 11(1), 10–18.

International Biometric Group (2008a). Analysis of Level 3 Features at High Resolutions, Phase II - Final Report.

International Biometric Group (2008b). L3TK - Level 3 Fingerprint Image Toolkit. Disponível em: <`http://level3tk.sourceforge.net`>. Acessado em: 26 jul. 2010.

Jain, A., Chen, Y., & Demirkus, M. (2006). Pores and ridges: Fingerprint matching using level 3 features. In *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, volume 4 (pp. 477–480).

Jain, A., Chen, Y., & Demirkus, M. (2007). Pores and ridges: High-resolution fingerprint matching using level 3 features. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(1), 15–27.

Jain, A., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1), 4–20.

Jain, A. K., Flynn, P., & Ross, A. A. (2008). *Handbook of Biometrics*. Secaucus, NJ, USA: Springer-Verlag New York, Inc.

Jain, A. K. & Maltoni, D. (2009). *Handbook of Fingerprint Recognition*. Secaucus, NJ, USA: Springer-Verlag New York, Inc.

Keerthi, S., Shevade, S., Bhattacharyya, C., & Murthy, K. (2001). Improvements to platt's smo algorithm for svm classifier design. *Neural Computation*, 13(3), 637–649.

Marasco, E. & Sansone, C. (2010). An anti-spoofing technique using multiple textural features in fingerprint scanners. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010 IEEE Workshop on* (pp. 8–14).

Marcialis, G., Lewicke, A., Tan, B., Coli, P., Grimberg, D., Congiu, A., Tidu, A., Roli, F., & Schuckers, S. (2009). First international fingerprint liveness detection competition - livdet 2009. In P. Foggia, C. Sansone, & M. Vento (Eds.), *Image Analysis and Processing ICIAP 2009*, volume 5716 of *Lecture Notes in Computer Science* (pp. 12–23). Springer Berlin Heidelberg.

Marcialis, G., Roli, F., & Tidu, A. (2010). Analysis of fingerprint pores for vitality detection. In *Pattern Recognition (ICPR), 2010 20th International Conference on* (pp. 1289–1292).

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial "gummy"fingers on fingerprint systems.

Nikam, S. & Agarwal, S. (2008). Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems. In *Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on* (pp. 675–680).

Papa, J. P., Falcão, A. X., & Suzuki, C. T. N. (2009). Supervised pattern classification based on optimum-path forest. *International Journal of Imaging Systems and Technology*, 19, 120–131.

Parthasaradhi, S., Derakhshani, R., Hornak, L., & Schuckers, S. A. C. (2005). Time-series detection of perspiration as a liveness test in fingerprint devices. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 35(3), 335–343.

Pereira, L., Pinheiro, H., Silva, J., Silva, A., Pina, T., Cavalcanti, G. D. C., Ren, T. I., & de Oliveira, J. (2012). A fingerprint spoof detection based on MLP and SVM. In *Neural Networks (IJCNN), The 2012 International Joint Conference on* (pp. 1–7).

Ratha, N., Connell, J., & Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634.

Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage and organization in the brain. *Psychological Review*, 65(6), 386–408.

Tabassi, E., Wilson, C. L., & Watson, C. I. (2004). *Fingerprint Image Quality (NFIQ)*. Technical Report NISTIR-7151, National Institute of Standards and Technology NIST.

Tan, B. & Schuckers, S. (2005). Liveness detection using an intensity based approach in fingerprint scanner. In *Proceedings of Biometrics Symposium, Arlington, VA (September 2005)*.

Tribunal Superior Eleitoral (2014). Recadastramento biométrico ultrapassa 64% da meta da justiça eleitoral. Disponível em: http://www.tse.jus.br/noticias-tse/2014/Janeiro/recadastramento-biometrico-ultrapassa-64-da-meta-da-justica-eleitoral. Acessado em: 10 janeiro 2014.

Yambay, D., Ghiani, L., Denti, P., Marcialis, G., Roli, F., & Schuckers, S. (2012). Livdet 2011 fingerprint liveness detection competition 2011. In *Biometrics (ICB), 2012 5th IAPR International Conference on* (pp. 208–215).

Zhao, Q. (2010). *High Resolution Fingerprint Additional Features Analysis*. PhD thesis, The Hong Kong Polytechnic University, Hong Kong.

Zhao, Q., Zhang, D., Zhang, D., Luo, N., & Bao, J. (2008). Adaptive pore model for fingerprint pore extraction. In *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1–4).

Zhao, Q., Zhang, D., Zhang, L., & Luo, N. (2010a). Adaptive fingerprint pore modeling and extraction. *Pattern Recognition*, 43(8), 2833 – 2844.

Zhao, Q., Zhang, D., Zhang, L., & Luo, N. (2010b). High Resolution Partial Fingerprint Alignment Using Pore-Valley Descriptors. *Pattern Recognition*, 43, 1050–1061.

Apêndice A

Parâmetros Utilizados

Tabela A.1: Classificadores e respectivos parâmetros utilizados na plataforma WEKA.

Tipo	Nome Classificador	Nome WEKA	Parâmetros
Function	SVM (Support Vector Machine)	functions.SMO	-C (10)
			-L (0.001)
			-P (1.0E-12)
			-N (0)
			-V (-1)
			-W (1)
			-K (Puk -O 1.0 -S 1.0 -C 250007)
	MLP (Multilayer Perceptron)	functions.MultilayerPerceptron	-L (0.3)
			-M (0.2)
			-N (500)
			-V (0)
			-S (0)
			-E (20)
			-H (a)
Lazy	kNN (k-Nearest Neighbors)	lazy.IBk	-K (1)
			-W (0)
			-A (EuclideanDistance -R first-last)
Tree	OPF (Optimum-Path Forest)	tree.OPF	-D (EuclideanDistance -R first-last)

Tabela A.2: Parâmetros de pré-processamento utilizados pelo método isotrópico (International Biometric Group, 2008a).

Parâmetro	Descrição	Valor
ip_macroblocksizeperdpi	Tamanho dos blocos (em pixels) sobre os quais a orientação do fluxo das cristas é determinado (proporção por dpi)	0.015 (Default)
ip_gaussianvarianceperdpi	Variância do *kernel* gaussiano usando para borramento da imagem (proporção por dpi)	0.001 (Default)
ip_uppercontrastthresh	Limiar com o qual os pixels com uma intensidade maior são alterados para 255 (setados como vales)	0.85 (Default)
ip_lowercontrastthresh	Limiar com o qual os pixels com uma intensidade inferior são alterados para 0 (setados como cristas)	0.15 (Default)

Tabela A.3: Parâmetros de extração de poros utilizados pelo método isotrópico (International Biometric Group, 2008a).

Parâmetro	**Descrição**	**Valor**
pe_minimumblobsizeperdpi	Menor tamanho dos poros que serão detectados a partir de "bolhas" na imagem (proporção por dpi)	0.00 (Default)
pe_maximumblobsizeperdpi	Maior tamanho dos poros que serão detectados a partir de "bolhas" na imagem (proporção por dpi)	0.045 (Default) 0.020 (Utilizado)
pe_mexhatvariance	Variância do *kernel* 2D da *wavelet* chapéu mexicano	2.6 (Default)
pe_mexhatthreshold	Limiar de intensidade com o qual a imagem processada pela *wavelet* chapéu mexicano é limiarizada	192 (Default) 120 (Utilizado)
pe_borderperdpi	Tamanho da borda, a qual é aplicada na imagem para remover ruídos introduzidos pelos vários passos de processamento (proporção por dpi)	0.005 (Default)

Tabela A.4: Parâmetros de extração de poros utilizados pelo método adaptativo (Zhao et al., 2010a).

Parâmetro	**Descrição**	**Valor**
IntensityStdThreshold	Limiar aplicado à intensidade de contraste do bloco, para classificação do mesmo	0.1
OrientationCertaintyThreshold	Limiar aplicado ao nível de certeza da orientação da crista obtida no bloco, para classificação do mesmo	0.2
SmallGaussianSigmaFactor	Tamanho da janela com o filtro gaussiano menor, a partir do qual é calculada sua variância (utilizado no filtro isotrópico baseado em DoG)	1/8
BigGaussianSigmaFactor	Tamanho da janela com o filtro gaussiano maior, a partir do qual é calculada sua variância (utilizado no filtro isotrópico baseado em DoG)	1/2
ThresholdSmallGaussian	Limiar aplicado sobre a imagem realçada pelo filtro gaussiano menor (utilizado no filtro isotrópico baseado em DoG)	0.01
ThresholdBigGaussian	Limiar aplicado sobre a imagem realçada pelo filtro gaussiano maior (utilizado no filtro isotrópico baseado em DoG)	0.05
APMSizeFactor	Fator multiplicado pela orientação para definição dos parâmetros do filtro DAPM	1/12
APMThreshold	Limiar aplicado sobre o bloco processado pelo filtro DAPM	0.5
MinPoreSize	Tamanho mínimo dos poros (em pixels), adotado na etapa de pós-processamento a fim de remover poros espúrios	5
MaxPoreSize	Tamanho máximo dos poros (em pixels), adotado na etapa de pós-processamento a fim de remover poros espúrios	30
GrayValuePercentage	Parâmetro de pós-processamento, para remoção de poros espúrios DAPM	0.2

Apêndice B

Resultados Completos

Para facilitar o entendimento dos resultados obtidos com este trabalho na Seção 5 foram apresentados apenas os resultados mais relevantes para as análises efetuadas. Neste apêndice estão apresentados todos os resultados obtidos com os demais classificadores e com os dois protocolos definidos para avaliação dos resultados. Esses resultados estão nas seguintes tabelas:

- **Tabela: B.1**: Resultados obtidos para base de dados LivDet 2013 utilizando o protocolo Cross Validation como descrito na Seção 4.3.1;
- **Tabela: B.2**: Resultados obtidos para base de dados LivDet 2013 utilizando o protocolo de Treinamento / Teste como descrito na Seção 4.3.1;
- **Tabela: B.3**: Resultados obtidos para base de dados UNESP-FSDB para imagens com 1000dpi utilizando o protocolo Cross Validation como descrito na Seção 4.3.1;
- **Tabela: B.4**: Resultados obtidos para base de dados UNESP-FSDB para imagens com 1000dpi utilizando protocolo de Treinamento / Teste como descrito na Seção 4.3.1;
- **Tabela: B.5**: Resultados obtidos para base de dados UNESP-FSDB para imagens com 500dpi utilizando o protocolo Cross Validation como descrito na Seção 4.3.1;
- **Tabela: B.6**: Resultados obtidos para base de dados UNESP-FSDB para imagens com 500dpi utilizando protocolo de Treinamento / Teste como descrito na Seção 4.3.1;

Tabela B.1: Resultados obtidos para base de dados LivDet 2013 utilizando o protocolo Cross Validation

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset Biometrika Test All Features	2000	52,00	48,00	96,00	0,00	48,00	91,90	8,10	7,80	8,40	8,10	52,00	48,00	96,00	0,00	48,00	93,30	6,70	6,50	6,90	6,70
Dataset Biometrika Test No Pores Information	2000	51,45	48,55	97,10	0,00	48,60	85,90	14,10	14,00	14,20	14,10	51,45	48,55	97,10	0,00	48,60	89,65	10,35	10,70	10,00	10,40
Dataset Biometrika Test Pores ROI 1	2000	51,75	48,25	96,50	0,00	48,30	88,40	11,60	9,80	13,40	11,60	51,75	48,25	96,50	0,00	48,30	90,90	9,10	8,00	10,20	9,10
Dataset Biometrika Test Pores ROI 2	2000	51,55	48,45	96,90	0,00	48,50	89,75	10,25	10,50	10,00	10,30	51,55	48,45	96,90	0,00	48,50	91,65	8,35	8,70	8,00	8,40
Dataset Biometrika Test Pores Whole	2000	51,55	48,45	96,90	0,00	48,50	89,75	10,25	10,50	10,00	10,30	51,55	48,45	96,90	0,00	48,50	91,65	8,35	8,70	8,00	8,40
Dataset Biometrika Test SM and Pores ROI 1	2000	51,90	48,10	96,20	0,00	48,10	90,65	9,35	9,90	8,80	9,40	51,90	48,10	96,20	0,00	48,10	92,75	7,25	7,30	7,20	7,30
Dataset Biometrika Test SM and Pores ROI 2	2000	51,55	48,45	96,90	0,00	48,50	91,65	8,35	9,60	7,10	8,40	51,55	48,45	96,90	0,00	48,50	94,25	5,75	5,40	6,10	5,80
Dataset Biometrika Test SM and Pores Whole	2000	51,55	48,45	96,90	0,00	48,50	91,65	8,35	9,60	7,10	8,40	51,55	48,45	96,90	0,00	48,50	94,25	5,75	5,40	6,10	5,80
Dataset Biometrika Test SM	2000	51,45	48,55	97,10	0,00	48,60	88,45	11,55	12,10	11,00	11,60	51,45	48,55	97,10	0,00	48,60	91,00	9,00	8,90	9,10	9,00
Dataset Biometrika Train All Features	2000	56,75	43,25	85,40	1,10	43,30	93,25	6,75	6,00	7,50	6,80	56,65	43,35	85,40	1,30	43,40	93,20	6,80	7,00	6,60	6,80
Dataset Biometrika Train No Pores Information	2000	52,75	47,25	93,50	1,00	47,30	87,70	12,30	13,40	11,20	12,30	52,70	47,30	93,50	1,10	47,30	89,10	10,90	11,70	10,10	10,90
Dataset Biometrika Train Pores ROI 1	2000	53,35	46,65	92,20	1,10	46,70	91,15	8,85	9,40	8,30	8,90	53,25	46,75	92,30	1,20	46,80	91,45	8,55	9,10	8,00	8,60
Dataset Biometrika Train Pores ROI 2	2000	54,05	45,95	90,60	1,30	46,00	91,20	8,80	8,70	8,90	8,80	53,95	46,05	90,80	1,30	46,10	91,95	8,05	7,80	8,30	8,10
Dataset Biometrika Train Pores Whole	2000	54,05	45,95	90,60	1,30	46,00	91,20	8,80	8,70	8,90	8,80	53,95	46,05	90,80	1,30	46,10	91,95	8,05	7,80	8,30	8,10
Dataset Biometrika Train SM and Pores ROI 1	2000	54,45	45,55	90,30	0,80	45,60	92,60	7,40	6,90	7,90	7,40	54,45	45,55	90,20	0,90	45,60	92,90	7,10	6,40	7,80	7,10
Dataset Biometrika Train SM and Pores ROI 2	2000	55,20	44,80	88,90	0,70	44,80	93,40	6,60	5,90	7,30	6,60	55,10	44,90	89,00	0,80	44,90	94,15	5,85	5,50	6,20	5,90
Dataset Biometrika Train SM and Pores Whole	2000	55,20	44,80	88,90	0,70	44,80	93,40	6,60	5,90	7,30	6,60	55,10	44,90	89,00	0,80	44,90	94,15	5,85	5,50	6,20	5,90
Dataset Biometrika Train SM	2000	54,10	45,90	90,80	1,00	45,90	90,25	9,75	9,30	10,20	9,80	54,10	45,90	90,80	1,00	45,90	90,05	9,95	10,80	9,10	10,00
Dataset Crossmatch Test All Features	2250	74,89	25,11	22,60	28,20	25,70	76,27	23,73	16,30	33,00	25,60	74,31	25,69	24,00	27,80	26,10	80,00	20,00	15,90	25,10	21,00
Dataset Crossmatch Test No Pores Information	2250	72,13	27,87	26,70	29,30	28,20	75,38	24,62	17,20	33,90	26,50	71,51	28,49	27,40	29,90	28,80	77,47	22,53	16,40	30,20	24,10
Dataset Crossmatch Test Pores ROI 1	2250	72,36	27,64	26,50	29,10	27,90	74,93	25,07	15,90	36,50	27,40	71,64	28,36	27,20	29,80	28,60	77,51	22,49	16,40	30,10	24,00
Dataset Crossmatch Test Pores ROI 2	2250	72,36	27,64	26,50	29,10	27,90	74,22	25,78	16,50	37,40	28,10	71,64	28,36	27,20	29,80	28,60	77,51	22,49	16,40	30,10	24,00
Dataset Crossmatch Test Pores Whole	2250	72,36	27,64	26,50	29,10	27,90	74,13	25,87	16,70	37,30	28,20	71,64	28,36	27,20	29,80	28,60	77,51	22,49	16,40	30,10	24,00
Dataset Crossmatch Test SM and Pores ROI 1	2250	74,89	25,11	22,60	28,20	25,70	76,58	23,42	16,60	32,00	25,10	74,31	25,69	24,00	27,80	26,10	80,00	20,00	15,90	25,10	21,00
Dataset Crossmatch Test SM and Pores ROI 2	2250	74,89	25,11	22,60	28,20	25,70	76,80	23,20	16,80	31,20	24,80	74,31	25,69	24,00	27,80	26,10	80,04	19,96	15,90	25,00	21,00
Dataset Crossmatch Test SM and Pores Whole	2250	74,89	25,11	22,60	28,20	25,70	76,80	23,20	17,30	30,60	24,70	74,31	25,69	24,00	27,80	26,10	80,00	20,00	15,90	25,10	21,00
Dataset Crossmatch Test SM	2250	74,84	25,16	22,60	28,30	25,80	77,78	22,22	15,70	30,40	23,90	74,27	25,73	24,00	27,90	26,20	80,00	20,00	15,90	25,10	21,00
Dataset Crossmatch Train All Features	2250	69,16	30,84	26,40	36,40	32,00	72,22	27,78	15,00	43,80	31,00	67,91	32,09	27,40	37,90	33,30	78,36	21,64	16,60	27,90	22,90
Dataset Crossmatch Train No Pores Information	2250	68,67	31,33	27,70	35,90	32,20	70,98	29,02	16,40	44,80	32,20	67,73	32,27	28,60	36,90	33,20	74,93	25,07	17,50	34,50	27,00
Dataset Crossmatch Train Pores ROI 1	2250	68,93	31,07	27,40	35,60	32,00	71,91	28,09	14,40	45,20	31,50	67,96	32,04	28,30	36,70	33,00	74,93	25,07	17,60	34,40	26,90
Dataset Crossmatch Train Pores ROI 2	2250	69,02	30,98	27,30	35,60	31,90	71,73	28,27	14,70	45,20	31,70	68,00	32,00	28,20	36,70	32,90	75,02	24,98	17,40	34,40	26,90
Dataset Crossmatch Train Pores Whole	2250	69,02	30,98	27,30	35,60	31,90	71,64	28,36	14,70	45,40	31,80	68,00	32,00	28,30	36,60	32,90	75,02	24,98	17,40	34,40	26,90
Dataset Crossmatch Train SM and Pores ROI 1	2250	69,07	30,93	26,60	36,40	32,00	72,98	27,02	15,60	41,30	29,90	67,82	32,18	27,60	37,90	33,30	78,22	21,78	16,70	28,10	23,00
Dataset Crossmatch Train SM and Pores ROI 2	2250	69,16	30,84	26,40	36,40	32,00	73,24	26,76	14,50	42,10	29,80	67,87	32,13	27,50	37,90	33,30	78,36	21,64	16,60	27,90	22,90
Dataset Crossmatch Train SM and Pores Whole	2250	69,16	30,84	26,40	36,40	32,00	72,98	27,02	14,20	43,00	30,20	67,87	32,13	27,60	37,80	33,30	78,36	21,64	16,60	27,90	22,90
Dataset Crossmatch Train SM	2250	68,67	31,33	26,90	36,90	32,40	72,62	27,38	15,70	42,00	30,30	67,38	32,62	28,00	38,40	33,80	78,09	21,91	17,10	27,90	23,10
Dataset Italdata Test All Features	2000	84,95	15,05	13,20	16,90	15,10	87,70	12,30	12,30	12,30	12,30	84,35	15,65	13,40	17,90	15,70	91,00	9,00	9,30	8,70	9,00
Dataset Italdata Test No Pores Information	2000	75,55	24,45	25,60	23,30	24,50	80,35	19,65	22,60	16,70	19,70	74,90	25,10	26,10	24,10	25,10	84,15	15,85	16,80	14,90	15,90
Dataset Italdata Test Pores ROI 1	2000	79,25	20,75	17,20	24,30	20,80	84,65	15,35	15,80	14,90	15,40	78,40	21,60	18,10	25,10	21,60	89,05	10,95	12,00	9,90	11,00
Dataset Italdata Test Pores ROI 2	2000	81,25	18,75	15,90	21,60	18,80	84,70	15,30	16,90	13,70	15,30	80,75	19,25	16,70	21,80	19,30	89,45	10,55	11,70	9,40	10,60
Dataset Italdata Test Pores Whole	2000	81,50	18,50	15,80	21,20	18,50	85,80	14,20	14,20	14,20	14,20	80,65	19,35	17,00	21,70	19,40	90,00	10,00	11,00	9,00	10,00
Dataset Italdata Test SM and Pores ROI 1	2000	84,10	15,90	12,90	18,90	15,90	86,30	13,70	12,50	14,90	13,70	83,15	16,85	13,70	20,00	16,90	90,35	9,65	10,10	9,20	9,70
Dataset Italdata Test SM and Pores ROI 2	2000	85,10	14,90	12,90	16,90	14,90	87,95	12,05	10,80	13,30	12,10	84,35	15,65	13,20	18,10	15,70	91,55	8,45	8,90	8,00	8,50
Dataset Italdata Test SM and Pores Whole	2000	85,20	14,80	12,40	17,20	14,80	87,65	12,35	12,50	12,20	12,40	84,60	15,40	12,90	17,90	15,40	92,05	7,95	8,20	7,70	8,00
Dataset Italdata Test SM	2000	80,70	19,30	22,70	15,90	19,30	83,60	16,40	16,00	16,80	16,40	79,95	20,05	23,50	16,60	20,10	87,40	12,60	14,20	11,00	12,60
Dataset Italdata Train All Features	2000	76,00	24,00	13,00	35,00	24,00	87,95	12,05	14,80	9,30	12,10	75,10	24,90	14,00	35,80	24,90	89,65	10,35	12,50	8,20	10,40
Dataset Italdata Train No Pores Information	2000	62,60	37,40	22,80	52,00	37,40	76,30	23,70	18,50	28,90	23,70	62,35	37,65	23,90	51,40	37,70	80,75	19,25	20,80	17,70	19,30
Dataset Italdata Train Pores ROI 1	2000	66,50	33,50	19,80	47,20	33,50	79,05	20,95	25,20	16,70	21,00	66,45	33,55	20,10	47,00	33,60	83,60	16,40	18,10	14,70	16,40
Dataset Italdata Train Pores ROI 2	2000	67,45	32,55	17,40	47,70	32,60	78,90	21,10	25,60	16,60	21,10	67,10	32,90	17,80	48,00	32,90	84,25	15,75	17,40	14,10	15,80
Dataset Italdata Train Pores Whole	2000	67,25	32,75	18,30	47,20	32,80	79,80	20,20	24,30	16,10	20,20	67,00	33,00	18,90	47,10	33,00	84,15	15,85	17,60	14,10	15,90
Dataset Italdata Train SM and Pores ROI 1	2000	76,60	23,40	12,60	34,20	23,40	87,85	12,15	14,10	10,20	12,20	75,80	24,20	13,50	34,90	24,20	89,60	10,40	12,00	8,80	10,40
Dataset Italdata Train SM and Pores ROI 2	2000	76,50	23,50	12,30	34,70	23,50	87,40	12,60	15,60	9,60	12,60	75,55	24,45	13,10	35,80	24,50	89,50	10,50	12,60	8,40	10,50
Dataset Italdata Train SM and Pores Whole	2000	76,60	23,40	12,30	34,50	23,40	87,20	12,80	16,00	9,60	12,80	75,85	24,15	13,00	35,30	24,20	89,45	10,55	12,70	8,40	10,60
Dataset Italdata Train SM	2000	76,75	23,25	16,60	29,90	23,30	85,20	14,80	16,50	13,10	14,80	75,75	24,25	18,20	30,30	24,30	87,80	12,20	14,10	10,30	12,20

Tabela B.2: Resultados obtidos para base de dados LivDet 2013 utilizando o protocolo Treinamento / Teste

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset Biometrika Train/Test All Features	2000	55,85	44,15	87,40	0,90	44,20	82,00	18,00	3,20	32,80	18,00	55,35	44,65	85,90	3,40	44,70	81,70	18,30	7,50	29,10	18,30
Dataset Biometrika Train/Test No Pores Information	2000	54,15	45,85	91,60	0,10	45,90	82,25	17,75	11,00	24,50	17,80	54,55	45,45	90,80	0,10	45,50	79,80	20,20	14,70	25,70	20,20
Dataset Biometrika Train/Test Pores ROI 1	2000	54,30	45,70	91,20	0,20	45,70	80,40	19,60	16,70	22,50	19,60	54,40	45,60	90,60	0,60	45,60	79,45	20,55	19,40	21,70	20,60
Dataset Biometrika Train/Test Pores ROI 2	2000	54,75	45,25	90,30	0,20	45,30	82,10	17,90	12,00	23,80	17,90	55,00	45,00	89,30	0,70	45,00	78,00	22,00	20,10	23,90	22,00
Dataset Biometrika Train/Test Pores Whole	2000	54,75	45,25	90,30	0,20	45,30	82,10	17,90	12,00	23,80	17,90	55,00	45,00	89,30	0,70	45,00	78,00	22,00	20,10	23,90	22,00
Dataset Biometrika Train/Test SM and Pores ROI 1	2000	54,85	45,15	90,00	0,30	45,20	81,90	18,10	5,90	30,30	18,10	55,35	44,65	88,50	0,80	44,70	81,45	18,55	7,60	29,50	18,60
Dataset Biometrika Train/Test SM and Pores ROI 2	2000	55,00	45,00	89,70	0,30	45,00	82,70	17,30	5,20	29,40	17,30	55,65	44,35	87,50	1,20	44,40	82,55	17,45	7,00	27,90	17,50
Dataset Biometrika Train/Test SM and Pores Whole	2000	55,00	45,00	89,70	0,30	45,00	82,70	17,30	5,20	29,40	17,30	55,65	44,35	87,50	1,20	44,40	82,55	17,45	7,00	27,90	17,50
Dataset Biometrika Train/Test SM	2000	54,60	45,40	90,50	0,30	45,40	78,75	21,25	3,60	38,90	21,30	55,35	44,65	89,00	0,30	44,70	78,90	21,10	5,80	36,40	21,10
Dataset Crossmatch Train/Test All Features	2250	62,58	37,42	29,40	47,50	39,40	66,53	33,47	7,10	66,40	40,10	62,00	38,00	30,20	47,80	40,00	64,71	35,29	24,40	48,90	38,00
Dataset Crossmatch Train/Test No Pores Information	2250	61,69	38,31	28,60	50,50	40,70	65,24	34,76	7,00	69,40	41,70	60,84	39,16	29,90	50,70	41,50	62,27	37,73	25,50	53,00	40,80
Dataset Crossmatch Train/Test Pores ROI 1	2250	61,69	38,31	28,60	50,40	40,70	65,29	34,71	3,80	73,30	42,40	60,76	39,24	30,10	50,70	41,50	62,04	37,96	25,90	53,00	41,00
Dataset Crossmatch Train/Test Pores ROI 2	2250	61,69	38,31	28,60	50,40	40,70	65,38	34,62	3,60	73,40	42,40	60,76	39,24	30,10	50,70	41,50	62,22	37,78	25,60	53,00	40,80
Dataset Crossmatch Train/Test Pores Whole	2250	61,69	38,31	28,60	50,40	40,70	65,38	34,62	3,60	73,40	42,40	60,76	39,24	30,10	50,70	41,50	62,18	37,82	25,70	53,00	40,90
Dataset Crossmatch Train/Test SM and Pores ROI 1	2250	62,58	37,42	29,40	47,50	39,40	68,93	31,07	11,50	55,50	36,00	62,00	38,00	30,20	47,80	40,00	64,62	35,38	24,60	48,90	38,10
Dataset Crossmatch Train/Test SM and Pores ROI 2	2250	62,58	37,42	29,40	47,50	39,40	68,76	31,24	11,40	56,00	36,20	62,00	38,00	30,20	47,80	40,00	64,67	35,33	24,50	48,90	38,00
Dataset Crossmatch Train/Test SM and Pores Whole	2250	62,58	37,42	29,40	47,50	39,40	68,89	31,11	11,40	55,80	36,00	62,00	38,00	30,20	47,80	40,00	64,67	35,33	24,50	48,90	38,00
Dataset Crossmatch Train/Test SM	2250	62,36	37,64	29,30	48,10	39,70	67,20	32,80	8,90	62,70	38,80	61,87	38,13	30,00	48,30	40,20	64,58	35,42	24,00	49,70	38,30
Dataset Italdata Train/Test All Features	2000	75,70	24,30	8,70	39,90	24,30	78,70	21,30	4,90	37,70	21,30	74,50	25,50	10,20	40,80	25,50	78,95	21,05	7,60	34,50	21,10
Dataset Italdata Train/Test No Pores Information	2000	62,45	37,55	17,80	57,30	37,60	70,00	30,00	15,50	44,50	30,00	61,40	38,60	19,90	57,30	38,60	73,15	26,85	20,00	33,70	26,90
Dataset Italdata Train/Test Pores ROI 1	2000	69,65	30,35	17,50	43,20	30,40	74,65	25,35	21,10	29,60	25,40	68,35	31,65	18,50	44,80	31,70	77,85	22,15	18,00	26,30	22,20
Dataset Italdata Train/Test Pores ROI 2	2000	68,00	32,00	14,50	49,50	32,00	72,65	27,35	20,10	34,60	27,40	67,25	32,75	15,10	50,40	32,80	78,40	21,60	16,30	26,90	21,60
Dataset Italdata Train/Test Pores Whole	2000	68,40	31,60	14,30	48,90	31,60	73,35	26,65	17,60	35,70	26,70	67,10	32,90	15,90	49,90	32,90	78,15	21,85	16,40	27,30	21,90
Dataset Italdata Train/Test SM and Pores ROI 1	2000	75,90	24,10	10,00	38,20	24,10	77,20	22,80	5,20	40,40	22,80	75,25	24,75	10,60	38,90	24,80	78,80	21,20	8,60	33,80	21,20
Dataset Italdata Train/Test SM and Pores ROI 2	2000	75,35	24,65	8,20	41,10	24,70	79,30	20,70	5,90	35,50	20,70	74,80	25,20	8,90	41,50	25,20	78,85	21,15	7,70	34,60	21,20
Dataset Italdata Train/Test SM and Pores Whole	2000	75,50	24,50	8,30	40,70	24,50	76,70	23,30	5,50	41,10	23,30	74,70	25,30	9,40	41,20	25,30	78,90	21,10	7,70	34,50	21,10
Dataset Italdata Train/Test SM	2000	70,00	30,00	11,90	48,10	30,00	73,05	26,95	6,60	47,30	27,00	70,15	29,85	12,10	47,60	29,90	74,65	25,35	10,10	40,60	25,40

Tabela B.3: Resultados obtidos para imagens com 1000dpi utilizando o protocolo Cross Validation

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset DRY 1000 1,2,3 Seg	720	88,06	11,94	23,30	6,30	17,60	90,56	9,44	14,60	6,90	12,00	86,94	13,06	25,40	6,90	19,20	91,81	8,19	15,00	4,80	11,60
Dataset DRY 1000 4,5,6 Seg	720	93,89	6,11	11,30	3,50	8,70	94,31	5,69	6,30	5,40	6,00	94,31	5,69	9,20	4,00	7,40	96,25	3,75	4,60	3,30	4,20
Dataset DRY 1000 7,8,9,10 Seg	960	95,73	4,27	6,60	3,10	5,40	97,50	2,50	3,80	1,90	3,10	95,21	4,79	8,40	3,00	6,60	98,02	1,98	3,80	1,10	2,90
Dataset DRY 1000 High Pressure	1200	97,33	2,67	6,50	0,80	4,60	97,25	2,75	5,00	1,60	3,90	96,58	3,42	7,50	1,40	5,50	97,92	2,08	5,00	0,60	3,50
Dataset DRY 1000 No Pores	2400	88,54	11,46	20,50	6,90	16,00	83,46	16,54	36,90	6,40	26,70	88,54	11,46	19,30	7,60	15,40	89,46	10,54	18,00	6,80	14,30
Dataset DRY 1000 Normal Pressure	1200	95,83	4,17	8,00	2,30	6,10	95,75	4,25	6,50	3,10	5,40	94,92	5,08	11,00	2,10	8,00	96,75	3,25	6,80	1,50	5,00
Dataset DRY 1000 Pores ROI 1	2400	91,21	8,79	16,00	5,20	12,40	89,92	10,08	15,90	7,20	13,00	90,50	9,50	16,00	6,30	12,80	92,17	7,83	13,40	5,10	10,60
Dataset DRY 1000 Pores ROI 2	2400	92,00	8,00	13,80	5,10	10,90	93,50	6,50	13,60	2,90	10,10	90,92	9,08	15,50	5,90	12,30	92,88	7,13	12,30	4,60	9,70
Dataset DRY 1000 Pores Whole	2400	93,21	6,79	11,80	4,30	9,30	91,67	8,33	17,90	3,60	13,10	92,54	7,46	12,60	4,90	10,00	93,33	6,67	11,80	4,10	9,20
Dataset DRY 1000 SM and Pores ROI 1	2400	93,75	6,25	11,50	3,60	8,90	92,67	7,33	15,40	3,30	11,40	93,04	6,96	12,40	4,30	9,70	94,71	5,29	9,90	3,00	7,60
Dataset DRY 1000 SM and Pores ROI 2	2400	93,58	6,42	13,10	3,10	9,80	93,17	6,83	13,90	3,30	10,40	93,25	6,75	13,10	3,60	9,90	95,33	4,67	8,80	2,60	6,70
Dataset DRY 1000 SM and Pores Whole	2400	94,38	5,63	9,90	3,50	7,80	91,88	8,13	13,10	5,60	10,60	93,88	6,13	11,80	3,30	8,90	95,29	4,71	9,30	2,40	7,00
Dataset DRY 1000 SM	2400	91,92	8,08	15,60	4,30	11,90	91,04	8,96	19,00	3,90	14,00	91,33	8,67	15,80	5,10	12,20	93,21	6,79	14,00	3,20	10,40
Dataset DRY 1000 Without 1 Seg	2160	97,92	2,08	3,90	1,20	3,00	97,08	2,92	6,10	1,30	4,50	97,41	2,59	5,10	1,30	3,90	98,38	1,62	3,80	0,60	2,70
Dataset DRY 1000	2400	96,54	3,46	6,30	2,10	4,90	95,33	4,67	8,40	2,80	6,50	96,21	3,79	7,10	2,10	5,50	97,83	2,17	4,40	1,10	3,30
Dataset WET 1000 1,2,3 Seg	720	97,22	2,78	4,20	2,10	3,50	98,89	1,11	2,90	0,20	2,00	97,78	2,22	4,20	1,30	3,20	98,61	1,39	2,10	1,00	1,70
Dataset WET 1000 4,5,6 Seg	720	99,58	0,42	0,80	0,20	0,60	99,44	0,56	1,30	0,20	0,90	98,89	1,11	2,10	0,60	1,60	99,58	0,42	0,80	0,20	0,60
Dataset WET 1000 7,8,9,10 Seg	960	99,27	0,73	0,60	0,80	0,70	99,69	0,31	0,00	0,50	0,20	98,85	1,15	1,90	0,80	1,50	99,69	0,31	0,60	0,20	0,50
Dataset WET 1000 High Pressure	1200	99,50	0,50	1,00	0,30	0,80	99,75	0,25	0,50	0,10	0,40	99,25	0,75	1,30	0,50	1,00	99,75	0,25	0,30	0,30	0,30
Dataset WET 1000 No Pores	2400	97,83	2,17	3,40	1,60	2,80	98,50	1,50	3,30	0,60	2,40	97,67	2,33	3,40	1,80	2,90	98,67	1,33	2,80	0,60	2,00
Dataset WET 1000 Normal Pressure	1200	99,83	0,17	0,30	0,10	0,20	99,58	0,42	1,30	0,00	0,80	99,50	0,50	1,00	0,30	0,80	99,83	0,17	0,30	0,10	0,20
Dataset WET 1000 Pores ROI 1	2400	97,92	2,08	3,40	1,40	2,70	99,00	1,00	1,90	0,60	1,40	97,75	2,25	3,30	1,80	2,80	98,63	1,38	2,80	0,70	2,10
Dataset WET 1000 Pores ROI 2	2400	98,54	1,46	2,80	0,80	2,10	99,67	0,33	0,90	0,10	0,60	98,58	1,42	1,90	1,20	1,60	99,42	0,58	0,90	0,40	0,70
Dataset WET 1000 Pores Whole	2400	99,08	0,92	1,40	0,70	1,10	99,08	0,92	2,00	0,40	1,50	98,88	1,13	1,60	0,90	1,40	99,38	0,63	1,00	0,40	0,80
Dataset WET 1000 SM and Pores ROI 1	2400	98,96	1,04	1,60	0,80	1,30	99,67	0,33	0,80	0,10	0,50	98,83	1,17	1,80	0,90	1,50	99,04	0,96	1,50	0,70	1,20
Dataset WET 1000 SM and Pores ROI 2	2400	99,08	0,92	1,80	0,50	1,30	99,75	0,25	0,60	0,10	0,40	98,58	1,42	2,10	1,10	1,80	99,50	0,50	1,00	0,30	0,80
Dataset WET 1000 SM and Pores Whole	2400	99,29	0,71	1,00	0,60	0,90	99,54	0,46	1,30	0,10	0,90	99,42	0,58	1,00	0,40	0,80	99,42	0,58	1,00	0,40	0,80
Dataset WET 1000 SM	2400	98,54	1,46	2,30	1,10	1,90	99,75	0,25	0,80	0,00	0,50	98,21	1,79	3,30	1,10	2,50	99,13	0,88	1,40	0,60	1,10
Dataset WET 1000 Without 1 Seg	2160	99,54	0,46	1,00	0,20	0,70	99,81	0,19	0,60	0,00	0,40	99,40	0,60	1,00	0,40	0,80	99,86	0,14	0,30	0,10	0,20
Dataset WET 1000	2400	99,42	0,58	0,80	0,50	0,70	99,71	0,29	0,60	0,10	0,50	99,13	0,88	1,40	0,60	1,10	99,58	0,42	0,60	0,30	0,50

Tabela B.4: Resultados obtidos para imagens com 1000dpi utilizando o protocolo Treinamento / Teste

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset DRY 1000 1,2,3 Seg	720	85,00	15,00	27,80	9,50	22,30	90,00	10,00	17,70	5,90	13,70	85,83	14,17	29,70	6,60	22,10	90,83	9,17	12,60	7,50	10,90
Dataset DRY 1000 4,5,6 Seg	720	93,06	6,94	10,20	5,60	8,80	91,67	8,33	8,10	8,50	8,20	88,61	11,39	20,30	7,00	16,00	94,44	5,56	11,80	2,50	8,70
Dataset DRY 1000 7,8,9,10 Seg	960	94,79	5,21	11,80	1,60	8,20	96,25	3,75	4,60	3,40	4,20	91,67	8,33	14,80	5,00	11,50	94,79	5,21	12,00	2,10	8,90
Dataset DRY 1000 High Pressure	1200	94,83	5,17	11,10	2,40	8,30	96,50	3,50	9,80	0,30	6,60	93,83	6,17	11,40	3,50	8,70	97,83	2,17	4,90	0,80	3,50
Dataset DRY 1000 No Pores	2400	85,58	14,42	22,20	10,80	18,50	83,42	16,58	35,20	7,30	25,80	86,08	13,92	23,40	9,00	18,50	87,67	12,33	20,80	8,00	16,50
Dataset DRY 1000 Normal Pressure	1200	94,67	5,33	7,90	4,10	6,70	94,00	6,00	7,40	5,30	6,70	92,17	7,83	13,40	5,00	10,60	96,67	3,33	7,40	1,30	5,30
Dataset DRY 1000 Pores ROI 1	2400	87,58	12,42	18,50	9,40	15,50	86,00	14,00	14,00	14,00	14,00	86,00	14,00	25,10	8,20	19,30	91,00	9,00	13,50	6,80	11,30
Dataset DRY 1000 Pores ROI 2	2400	89,58	10,42	19,60	5,70	14,90	93,50	6,50	13,50	3,40	10,40	86,08	13,92	22,60	9,50	18,10	91,08	8,92	15,70	5,50	12,30
Dataset DRY 1000 Pores Whole	2400	90,50	9,50	15,90	6,50	12,90	89,75	10,25	24,90	3,40	18,10	90,67	9,33	16,00	6,00	12,60	90,92	9,08	12,50	7,20	10,60
Dataset DRY 1000 SM and Pores ROI 1	2400	89,33	10,67	17,70	7,40	14,40	92,00	8,00	17,70	3,00	12,80	91,33	8,67	12,60	6,80	10,70	93,08	6,92	11,20	4,80	9,00
Dataset DRY 1000 SM and Pores ROI 2	2400	92,33	7,67	15,30	3,90	11,50	93,58	6,42	16,40	1,60	11,60	89,92	10,08	21,50	4,20	15,60	93,50	6,50	11,80	3,80	9,10
Dataset DRY 1000 SM and Pores Whole	2400	91,75	8,25	15,20	4,80	11,70	94,33	5,67	11,20	3,00	8,50	91,50	8,50	17,40	3,50	12,40	94,67	5,33	10,90	2,60	8,20
Dataset DRY 1000 SM	2400	91,00	9,00	20,50	3,50	15,00	91,92	8,08	14,70	5,00	11,60	88,92	11,08	19,70	6,20	14,80	92,67	7,33	14,40	4,00	11,10
Dataset DRY 1000 Without 1 Seg	2160	95,46	4,54	8,70	2,50	6,60	96,02	3,98	9,60	1,10	6,80	95,46	4,54	8,70	2,50	6,60	97,04	2,96	6,70	1,20	5,00
Dataset DRY 1000	2400	94,17	5,83	11,00	3,40	8,60	93,92	6,08	7,80	5,20	6,90	93,58	6,42	11,40	3,80	8,80	96,67	3,33	6,60	1,60	4,80
Dataset WET 1000 1,2,3 Seg	720	96,39	3,61	7,60	1,30	5,30	98,06	1,94	6,00	0,00	4,00	95,28	4,72	6,50	3,80	5,60	97,78	2,22	3,60	1,60	3,00
Dataset WET 1000 4,5,6 Seg	720	98,33	1,67	3,10	0,90	2,30	99,72	0,28	0,90	0,00	0,60	97,50	2,50	4,10	1,70	3,30	99,17	0,83	2,70	0,00	1,90
Dataset WET 1000 7,8,9,10 Seg	960	96,67	3,33	3,10	3,40	3,20	99,79	0,21	0,00	0,30	0,10	98,75	1,25	0,60	1,60	0,90	99,17	0,83	2,40	0,00	1,50
Dataset WET 1000 High Pressure	1200	99,33	0,67	0,00	1,00	0,30	99,83	0,17	0,50	0,00	0,30	97,50	2,50	3,50	2,00	3,00	99,33	0,67	0,50	0,80	0,60
Dataset WET 1000 No Pores	2400	96,42	3,58	4,60	3,10	4,10	98,25	1,75	4,70	0,40	3,30	96,42	3,58	4,90	3,00	4,30	97,83	2,17	3,70	1,40	2,90
Dataset WET 1000 Normal Pressure	1200	99,50	0,50	1,00	0,30	0,70	99,83	0,17	0,00	0,30	0,10	98,17	1,83	3,50	1,00	2,70	99,83	0,17	0,00	0,30	0,10
Dataset WET 1000 Pores ROI 1	2400	96,92	3,08	4,10	2,60	3,50	98,42	1,58	0,80	2,00	1,20	97,17	2,83	5,50	1,50	4,10	97,50	2,50	5,20	1,20	3,90
Dataset WET 1000 Pores ROI 2	2400	97,67	2,33	2,50	2,30	2,40	99,50	0,50	1,20	0,10	0,80	97,75	2,25	4,90	0,90	3,50	98,83	1,17	1,50	1,00	1,30
Dataset WET 1000 Pores Whole	2400	97,92	2,08	2,60	1,80	2,30	99,00	1,00	2,80	0,10	1,90	98,50	1,50	3,20	0,60	2,30	98,83	1,17	2,30	0,60	1,70
Dataset WET 1000 SM and Pores ROI 1	2400	98,17	1,83	2,60	1,50	2,20	99,75	0,25	0,00	0,40	0,10	97,83	2,17	3,00	1,70	2,60	98,75	1,25	2,40	0,60	1,80
Dataset WET 1000 SM and Pores ROI 2	2400	98,25	1,75	2,80	1,20	2,20	99,50	0,50	1,20	0,10	0,80	97,92	2,08	2,40	1,90	2,30	99,17	0,83	0,50	1,00	0,70
Dataset WET 1000 SM and Pores Whole	2400	99,58	0,42	0,50	0,40	0,50	98,58	1,42	4,10	0,00	2,70	98,67	1,33	2,00	1,00	1,70	98,92	1,08	2,00	0,60	1,60
Dataset WET 1000 SM	2400	98,17	1,83	3,70	0,90	2,80	99,08	0,92	1,20	0,80	1,00	98,00	2,00	3,40	1,30	2,70	99,17	0,83	2,00	0,30	1,40
Dataset WET 1000 Without 1 Seg	2160	99,07	0,93	0,30	1,30	0,60	99,63	0,37	1,10	0,00	0,70	98,98	1,02	2,00	0,50	1,50	99,91	0,09	0,30	0,00	0,20
Dataset WET 1000	2400	98,83	1,17	1,00	1,30	1,10	99,33	0,67	1,00	0,50	0,90	99,00	1,00	1,00	1,00	1,00	99,25	0,75	1,70	0,30	1,20

Tabela B.5: Resultados obtidos para imagens com 500dpi utilizando o protocolo Cross Validation

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset DRY 500 1,2,3 Seg	720	93,19	6,81	14,20	3,10	10,50	92,36	7,64	12,50	5,20	10,10	92,64	7,36	14,20	4,00	10,80	96,11	3,89	8,30	1,70	6,10
Dataset DRY 500 4,5,6 Seg	720	97,36	2,64	3,30	2,30	3,00	95,97	4,03	5,40	3,30	4,70	97,78	2,22	2,90	1,90	2,60	99,44	0,56	1,30	0,20	0,90
Dataset DRY 500 7,8,9,10 Seg	960	99,48	0,52	1,30	0,20	0,90	97,60	2,40	3,80	1,70	3,10	98,96	1,04	1,90	0,60	1,50	99,38	0,63	0,90	0,50	0,80
Dataset DRY 500 High Pressure	1200	98,08	1,92	4,80	0,50	3,30	97,50	2,50	5,00	1,30	3,80	98,00	2,00	4,50	0,80	3,30	98,42	1,58	3,50	0,60	2,50
Dataset DRY 500 No Pores	2400	90,04	9,96	17,30	6,30	13,60	84,88	15,13	33,40	6,00	24,30	89,33	10,67	18,60	6,70	14,60	88,29	11,71	23,90	5,60	17,80
Dataset DRY 500 Normal Pressure	1200	97,67	2,33	4,80	1,10	3,50	95,67	4,33	6,80	3,10	5,50	97,25	2,75	4,80	1,80	3,80	98,33	1,67	3,80	0,60	2,70
Dataset DRY 500 Pores ROI 1	2400	91,71	8,29	15,60	4,60	12,00	83,25	16,75	28,50	10,90	22,60	90,75	9,25	16,90	5,40	13,10	91,71	8,29	14,90	5,00	11,60
Dataset DRY 500 Pores ROI 2	2400	92,21	7,79	14,40	4,50	11,10	87,17	12,83	28,00	5,30	20,40	91,25	8,75	15,60	5,30	12,20	92,38	7,63	14,90	4,00	11,30
Dataset DRY 500 Pores Whole	2400	94,88	5,13	9,90	2,80	7,50	89,38	10,63	16,30	7,80	13,40	94,25	5,75	11,00	3,10	8,40	94,21	5,79	11,80	2,80	8,80
Dataset DRY 500 SM and Pores ROI 1	2400	95,63	4,38	7,30	2,90	5,80	90,79	9,21	17,40	5,10	13,30	95,04	4,96	7,80	3,60	6,40	97,92	2,08	3,90	1,20	3,00
Dataset DRY 500 SM and Pores ROI 2	2400	95,96	4,04	7,60	2,30	5,80	90,54	9,46	16,50	5,90	13,00	95,46	4,54	8,10	2,80	6,30	97,54	2,46	5,30	1,10	3,90
Dataset DRY 500 SM and Pores Whole	2400	97,58	2,42	4,80	1,30	3,60	93,54	6,46	12,80	3,30	9,60	96,96	3,04	5,60	1,80	4,30	97,50	2,50	5,90	0,80	4,20
Dataset DRY 500 SM	2400	95,50	4,50	8,30	2,60	6,40	92,83	7,17	12,50	4,50	9,80	95,08	4,92	8,90	2,90	6,90	96,58	3,42	7,80	1,30	5,60
Dataset DRY 500 Without 1 Seg	2160	99,12	0,88	1,10	0,80	1,00	96,57	3,43	6,50	1,90	5,00	98,61	1,39	2,10	1,00	1,70	99,40	0,60	0,80	0,50	0,70
Dataset DRY 500	2400	98,25	1,75	3,90	0,70	2,80	96,21	3,79	7,30	2,10	5,50	97,63	2,38	4,10	1,50	3,30	98,63	1,38	3,10	0,50	2,30
Dataset WET 500 1,2,3 Seg	720	97,08	2,92	4,60	2,10	3,80	97,22	2,78	5,80	1,30	4,30	97,22	2,78	5,00	1,70	3,90	97,36	2,64	3,80	2,10	3,20
Dataset WET 500 4,5,6 Seg	720	99,86	0,14	0,40	0,00	0,30	97,78	2,22	4,60	1,00	3,40	99,17	0,83	1,30	0,60	1,00	99,58	0,42	0,80	0,20	0,60
Dataset WET 500 7,8,9,10 Seg	960	99,69	0,31	0,60	0,20	0,50	98,23	1,77	3,10	1,10	2,40	99,48	0,52	0,90	0,30	0,70	100,00	0,00	0,00	0,00	0,00
Dataset WET 500 High Pressure	1200	99,42	0,58	1,00	0,40	0,80	99,58	0,42	1,00	0,10	0,70	99,42	0,58	1,30	0,30	0,90	99,42	0,58	1,00	0,40	0,80
Dataset WET 500 No Pores	2400	97,96	2,04	3,40	1,40	2,70	97,33	2,67	3,50	2,30	3,10	97,92	2,08	3,90	1,20	3,00	98,58	1,42	1,80	1,30	1,60
Dataset WET 500 Normal Pressure	1200	99,42	0,58	0,80	0,50	0,70	98,17	1,83	5,30	0,10	3,50	99,08	0,92	1,30	0,80	1,10	99,58	0,42	0,80	0,30	0,60
Dataset WET 500 Pores ROI 1	2400	98,13	1,88	3,10	1,30	2,50	97,75	2,25	3,30	1,80	2,80	97,79	2,21	3,50	1,60	2,90	98,88	1,13	2,40	0,50	1,80
Dataset WET 500 Pores ROI 2	2400	98,67	1,33	2,50	0,80	1,90	98,21	1,79	3,40	1,00	2,60	98,25	1,75	3,10	1,10	2,40	99,38	0,63	0,90	0,50	0,80
Dataset WET 500 Pores Whole	2400	99,29	0,71	1,50	0,30	1,10	97,92	2,08	4,50	0,90	3,30	99,04	0,96	2,10	0,40	1,50	99,29	0,71	1,60	0,30	1,20
Dataset WET 500 SM and Pores ROI 1	2400	98,50	1,50	2,60	0,90	2,10	97,21	2,79	5,00	1,70	3,90	98,25	1,75	3,00	1,10	2,40	99,21	0,79	1,90	0,30	1,30
Dataset WET 500 SM and Pores ROI 2	2400	98,92	1,08	1,80	0,80	1,40	97,83	2,17	3,40	1,60	2,80	98,54	1,46	2,10	1,10	1,80	99,38	0,63	1,10	0,40	0,90
Dataset WET 500 SM and Pores Whole	2400	99,29	0,71	1,60	0,30	1,20	97,75	2,25	4,90	0,90	3,60	99,21	0,79	1,80	0,30	1,30	99,42	0,58	1,50	0,10	1,00
Dataset WET 500 SM	2400	98,50	1,50	2,50	1,00	2,00	98,17	1,83	2,30	1,60	2,00	98,13	1,88	2,60	1,50	2,30	99,17	0,83	1,90	0,30	1,40
Dataset WET 500 Without 1 Seg	2160	99,77	0,23	0,30	0,20	0,30	98,80	1,20	3,10	0,30	2,10	99,72	0,28	0,40	0,20	0,30	99,77	0,23	0,40	0,10	0,30
Dataset WET 500	2400	99,38	0,63	1,10	0,40	0,90	98,46	1,54	4,00	0,30	2,80	99,17	0,83	1,60	0,40	1,20	99,46	0,54	1,00	0,30	0,80

Tabela B.6: Resultados obtidos para imagens com 500dpi utilizando o protocolo Treinamento / Teste

Dataset	Images	KNN					MLP					OPF					SVM				
		%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG	%Cor.	%Inc.	%FAR	%FRR	AVG
Dataset DRY 500 1,2,3 Seg	720	91,11	8,89	15,70	6,00	12,80	91,39	8,61	17,70	3,80	12,90	91,94	8,06	10,20	7,00	9,10	91,94	8,06	16,00	4,10	12,10
Dataset DRY 500 4,5,6 Seg	720	96,39	3,61	7,40	2,00	5,80	97,22	2,78	4,00	2,10	3,40	95,00	5,00	7,60	3,70	6,30	96,94	3,06	3,40	2,90	3,20
Dataset DRY 500 7,8,9,10 Seg	960	96,04	3,96	5,30	3,20	4,60	97,29	2,71	4,60	1,80	3,70	95,21	4,79	9,90	2,20	7,30	97,92	2,08	2,70	1,80	2,40
Dataset DRY 500 High Pressure	1200	97,00	3,00	6,80	1,20	5,10	96,83	3,17	6,40	1,50	4,70	96,67	3,33	7,40	1,30	5,30	98,67	1,33	2,50	0,80	1,90
Dataset DRY 500 No Pores	2400	88,67	11,33	23,50	5,10	17,20	85,83	14,17	23,70	9,90	19,40	86,50	13,50	22,60	8,80	17,90	86,58	13,42	24,20	8,00	18,80
Dataset DRY 500 Normal Pressure	1200	96,17	3,83	9,50	1,20	6,90	95,50	4,50	6,90	3,30	5,60	93,00	7,00	9,90	5,50	8,40	96,00	4,00	6,40	2,80	5,20
Dataset DRY 500 Pores ROI 1	2400	88,92	11,08	20,50	6,60	16,10	81,25	18,75	23,20	16,50	20,90	90,42	9,58	15,90	6,50	12,90	89,17	10,83	20,10	6,10	15,50
Dataset DRY 500 Pores ROI 2	2400	89,67	10,33	18,10	6,50	14,20	86,83	13,17	38,10	1,10	26,10	89,08	10,92	20,50	5,90	15,60	89,42	10,58	20,30	5,60	15,30
Dataset DRY 500 Pores Whole	2400	93,42	6,58	13,10	3,50	10,00	86,17	13,83	12,80	14,30	13,30	90,92	9,08	14,70	5,90	11,50	93,08	6,92	11,70	4,70	9,50
Dataset DRY 500 SM and Pores ROI 1	2400	94,67	5,33	9,90	3,20	7,80	88,92	11,08	21,00	6,50	16,40	93,92	6,08	11,00	3,60	8,50	96,42	3,58	7,80	1,30	5,50
Dataset DRY 500 SM and Pores ROI 2	2400	95,50	4,50	9,70	2,10	7,20	90,50	9,50	18,00	5,30	13,70	93,50	6,50	11,00	4,20	8,70	95,17	4,83	7,40	3,50	6,10
Dataset DRY 500 SM and Pores Whole	2400	96,00	4,00	7,00	2,50	5,50	92,83	7,17	15,60	2,60	11,00	94,92	5,08	8,80	3,20	6,80	96,67	3,33	7,90	1,10	5,70
Dataset DRY 500 SM	2400	93,75	6,25	10,40	4,30	8,50	90,08	9,92	26,00	1,50	17,60	92,50	7,50	13,30	4,50	10,20	95,25	4,75	8,20	2,80	6,30
Dataset DRY 500 Without 1 Seg	2160	97,96	2,04	3,60	1,20	2,80	96,94	3,06	8,00	0,60	5,50	96,67	3,33	2,80	3,60	3,10	97,69	2,31	6,50	0,40	4,50
Dataset DRY 500	2400	97,67	2,33	5,70	0,60	4,00	97,17	2,83	6,90	0,90	4,90	95,83	4,17	7,40	2,30	5,60	97,92	2,08	4,10	1,10	3,10
Dataset WET 500 1,2,3 Seg	720	95,28	4,72	9,20	2,20	6,60	98,06	1,94	5,10	0,40	3,60	94,17	5,83	13,00	2,10	9,30	97,22	2,78	3,60	2,40	3,20
Dataset WET 500 4,5,6 Seg	720	98,61	1,39	3,80	0,00	2,40	96,67	3,33	10,30	0,00	6,90	97,50	2,50	6,50	0,40	4,40	98,89	1,11	2,70	0,40	2,00
Dataset WET 500 7,8,9,10 Seg	960	99,58	0,42	1,20	0,00	0,80	98,13	1,88	3,10	1,30	2,50	98,13	1,88	5,10	0,30	3,50	99,38	0,63	1,80	0,00	1,10
Dataset WET 500 High Pressure	1200	99,17	0,83	2,50	0,00	1,60	97,17	2,83	3,80	2,30	3,30	98,50	1,50	3,00	0,80	2,20	98,67	1,33	2,30	0,80	1,70
Dataset WET 500 No Pores	2400	97,00	3,00	4,00	2,50	3,50	97,75	2,25	6,10	0,30	4,10	97,17	2,83	4,10	2,20	3,50	97,92	2,08	3,10	1,60	2,60
Dataset WET 500 Normal Pressure	1200	99,17	0,83	1,00	0,80	0,90	98,50	1,50	3,80	0,30	2,60	99,33	0,67	0,50	0,80	0,60	99,67	0,33	0,90	0,00	0,60
Dataset WET 500 Pores ROI 1	2400	96,92	3,08	5,50	1,90	4,30	97,33	2,67	4,50	1,70	3,50	97,17	2,83	5,40	1,50	4,10	98,08	1,92	3,80	1,00	2,90
Dataset WET 500 Pores ROI 2	2400	98,00	2,00	3,70	1,10	2,90	96,58	3,42	3,30	3,50	3,40	98,58	1,42	2,30	1,00	1,90	98,33	1,67	2,20	1,40	2,00
Dataset WET 500 Pores Whole	2400	98,42	1,58	4,10	0,30	2,70	97,92	2,08	5,30	0,50	3,70	98,42	1,58	3,50	0,60	2,50	99,42	0,58	1,60	0,10	1,10
Dataset WET 500 SM and Pores ROI 1	2400	98,25	1,75	3,10	1,00	2,40	96,75	3,25	5,10	2,30	4,10	97,42	2,58	5,40	1,30	4,10	99,08	0,92	2,20	0,30	1,60
Dataset WET 500 SM and Pores ROI 2	2400	98,00	2,00	3,60	1,20	2,80	97,17	2,83	5,40	1,60	4,20	97,75	2,25	3,10	1,80	2,70	99,17	0,83	2,00	0,30	1,40
Dataset WET 500 SM and Pores Whole	2400	98,83	1,17	2,10	0,70	1,60	98,08	1,92	4,80	0,40	3,20	98,92	1,08	2,00	0,60	1,60	99,17	0,83	1,90	0,30	1,30
Dataset WET 500 SM	2400	97,33	2,67	5,30	1,30	3,90	96,33	3,67	3,50	3,70	3,60	98,33	1,67	2,40	1,30	2,00	98,42	1,58	2,50	1,10	2,10
Dataset WET 500 Without 1 Seg	2160	99,44	0,56	0,50	0,60	0,50	97,78	2,22	4,10	1,30	3,20	98,98	1,02	2,90	0,10	2,00	99,35	0,65	1,30	0,30	1,00
Dataset WET 500	2400	99,08	0,92	1,20	0,80	1,10	98,00	2,00	3,60	1,20	2,70	99,58	0,42	0,30	0,50	0,30	99,08	0,92	2,00	0,40	1,40

Autorizo a reprodução xerográfica para fins de pesquisa.

São José do Rio Preto, 31/07/2015

Murilo V. Silva

Assinatura