

UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

DETECÇÃO DE IMPRESSÕES DIGITAIS
FRAUDULENTAS UTILIZANDO PADRÕES
MAPEADOS LOCALMENTE EM MULTIESCALA

RODRIGO COLNAGO CONTRERAS

ORIENTADOR: PROF. DR. MAURÍLIO BOAVENTURA

CO-ORIENTADOR: PROF.^a DR.^a INÊS APARECIDA GASPAROTTO BOAVENTURA

São José do Rio Preto - SP

Junho/2015

UNIVERSIDADE ESTADUAL PAULISTA

“JÚLIO DE MESQUITA FILHO”

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

**DETECÇÃO DE IMPRESSÕES DIGITAIS
FRAUDULENTAS UTILIZANDO PADRÕES
MAPEADOS LOCALMENTE EM MULTIESCALA**

RODRIGO COLNAGO CONTRERAS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para a obtenção do título de Mestre em Matemática, área de concentração: Modelagem Matemática.

Orientador: Prof. Dr. Maurílio Boaventura

São José do Rio Preto – SP

Junho/2015

Contreras, Rodrigo Colnago.

Detecção de impressões digitais fraudulentas utilizando padrões mapeados localmente em multiescala / Rodrigo Colnago Contreras. -- São José do Rio Preto, 2015

87 f. : il., tabs.

Orientador: Maurílio Boaventura

Coorientador: Inês Aparecida Gasparotto Boaventura

Dissertação (mestrado) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas

1. Computação - Matemática. 2. Modelos matemáticos. 3. Sistemas de detecção de intrusão (Medidas de segurança) 4. Biometria. 5. Reconhecimento de padrões. 6. Aprendizado do computador. I. Boaventura, Maurílio. II. Boaventura, Inês Aparecida Gasparotto. III. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. IV. Título.

CDU – 518.72

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

Dedico este trabalho aos meus avós.

AGRADECIMENTO

Gostaria de agradecer a todos que, de alguma forma, contribuíram para que este trabalho pudesse ser realizado. Em especial agradeço:

Ao professor Maurílio, que com muito talento e maestria me orientou durante vários anos, me propiciando um excelente amadurecimento científico. Agradeço pelas críticas, pela paciência e pela prestatividade na condução deste trabalho.

À professora Inês, pelas valiosas e decisivas dicas.

A toda minha família, principalmente aos meus pais, pelo imenso amor que recebo todos os dias, pelo apoio, incentivo e carinho, e por me fazerem sentir querido por pessoas tão especiais. Também agradeço pela contribuição moral que cada um deu na minha formação intelectual e de caráter.

A minha namorada Monique, que com muita paciência me tolera há quase 8 anos e ainda está “se acostumando ao meu jeito”. Agradeço também suas valiosas revisões dedicadas a este trabalho e ao amor e companheirismo dedicados a mim.

Aos meus queridos amigos Alex, Flávio e Robson, cujos nomes estão propositalmente dispostos em ordem alfabética, pelo companheirismo e amizade frente às mais diversas situações encaradas no decorrer desses anos de formação acadêmica. Agradeço também ao meu amigo Marcelo, cujas habilidades em Magic® deixam a desejar, e ao meu amigo Eric por sua venustidade exuberante.

À CAPES, pelo suporte financeiro.

Que coleção de cicatrizes você tem? Nunca se esqueça de quem lhe deu as melhores. E seja grato. Nossas cicatrizes têm o poder de nos fazer lembrar que o passado foi real.

Dr. Hannibal Lecter

Resumo

Aplicações que fazem uso de reconhecimento de impressões digitais estão presentes em muitos contextos do dia a dia, por exemplo, transações em caixas automáticos, registro eletrônico de ponto em empresas e, desde 2008, no processo eleitoral brasileiro. A comparação entre impressões digitais geralmente é feita com base nas posições relativas de pequenos padrões conhecidos como minúcias. Estudos científicos recentes demonstram a possibilidade de confecção de impressões digitais sintéticas, que apresentam a cópia das minúcias presentes em um dedo autêntico, a partir de materiais simples como massa de modelar, silicone, cola de madeira, dentre outros. Diante do perigo iminente de fraude em sistemas biométricos, surgiu uma nova linha de pesquisa: a detecção de impressões digitais fraudulentas (*spoofs*). Atualmente, estão presentes na literatura alguns métodos capazes de amenizar este problema, mas este ainda é um problema em aberto. O presente trabalho concentra-se na detecção de impressões digitais fraudulentas utilizando técnicas de processamento de imagens e reconhecimento de padrões. A principal contribuição desse estudo é uma nova técnica com a qual as falsificações são detectadas a partir da análise de micropadrões espaciais extraídos das impressões digitais. Além disso, é desenvolvida neste trabalho a versão multiescala do micropadrão espacial conhecido como Padrão Mapeado Localmente (*Local Mapped Pattern* - LMP). Os experimentos conduzidos mostraram que, através da técnica proposta, é possível alcançar uma detecção com performances superiores aos resultados encontrados no estado da arte na literatura científica especializada.

Palavras-chave: Biometria, Reconhecimento de Padrões, *Support Vector Machine*, Segurança de Sistemas, *Spoofing Fingerprints*, *Local Mapped Pattern*.

ABSTRACT

Applications which use fingerprint recognition are present in many contexts of everyday life, for example, transactions at ATMs, electronic registration point in companies and, since 2008, in the Brazilian electoral process. The fingerprint matching is usually made based on the relative positions of small patterns known as minutiae. Recent scientific researches show the possibility of making synthetic fingerprints, which have a copy of these minutiae in an authentic finger, from simple materials such as play dough, silicone, wood glue, among others. Faced with the imminent danger of fraud in biometric systems, a new line of research emerged: the detection of fake fingerprints (spoofs). Currently, they are in the literature some methods to minimize this problem, but this is still an open problem. The present study focuses on the detection of fake fingerprints using image processing and pattern recognition techniques. The main contribution of this study is a new technique with which the fakes one are detected from the analysis of spatial micro patterns extracted from the fingerprints. Moreover, it is developed in this work, the multi-scale version of the space micro pattern known as Local Mapped Pattern (LMP). The experiments carried out have shown that through the proposed technique, it is possible to achieve a higher detection performances with the results found state of the art in the specialized literature.

Keywords: Biometrics, Pattern Recognition, Support Vector Machine, System Security, Spoofing Fingerprints, Local Mapped Pattern.

LISTA DE FIGURAS

Figura 1.1 – Esquema de Autenticação. (a) Esquema tradicional utilizando Cartão de Identificação, senhas e chaves para validar o indivíduo e ter certeza que os recursos do sistema estão sendo acessados por um indivíduo legítimo. (b) Identificação com uso da biometria. Fonte: (JAIN; FLYNN; ROSS, 2007).	17
Figura 1.2– Dedos de silicone seriam utilizados por médicos e enfermeiros para fraudar ponto eletrônico. Fonte: (PEIXOTO; LOURENÇO, 2013).	18
Figura 1.3 – Representação do estado da arte das pesquisas de métodos de detecção de <i>spoof</i> . Adaptado de (AL-AJLAN, 2013).	20
Figura 1.4 – Diferenças de níveis de cinza como um padrão local. Fonte: (FERRAZ; JUNIOR; GONZAGA, 2014).	23
Figura 2.1 – Exemplo de impressão digital. Adaptado de (JAIN; FLYNN; ROSS, 2007).	28
Figura 2.2 – Exemplo de singularidade Delta. Impressão Digital de (GHIANI et al., 2013).	30
Figura 2.3 – Regiões singulares de Henry. (a) Verticilo, (b) Presilha Interna, (c) Presilha Externa, (d) Arco Plano, (e) Arco Angular. Adaptado de (MALTONI et al., 2009).	31
Figura 2.4 – Singularidades relativamente locais. (a) Bifurcação, (b) Terminação, (c) Lago, (d) Cruzamento, (e) Ponto, (f) Crista Independente e (g) Espora. Adaptado de (MALTONI et al., 2009).	32
Figura 2.5 – Ilustração do funcionamento geral de um sensor de impressões digitais. Adaptado de (MALTONI et al., 2009).	33
Figura 2.6 – 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 (MALTONI et al., 2009).	34
Figura 2.7 – Um exemplo de imagem com 500dpi capturada com um scanner multidedos <i>Papillon</i> DS-30, os quatro retângulos mostram a posição das quatro impressões digitais localizadas por um algoritmo de segmentação automática. Adaptado de (MALTONI et al., 2009).	34
Figura 2.8 – Representação funcional de um <i>Frustrated Total Internal Reflection</i> (FTIR). Adaptado de (SOUSEDIK; BUSCH, 2014).	35

Figura 2.9 – Representação funcional de um Sensor piezoelétrico. Adaptado de (SOUSEDIK; BUSCH, 2014).	36
Figura 2.10 – Exemplo de minúcias usadas para o <i>match</i> entre impressões digitais. (ASHBOURN, 2002).	36
Figura 2.11 – Oito pontos através dos quais um sistema de reconhecimento de impressões digitais pode ser atacado, permitindo, assim, a autenticação de indivíduos não autorizados. Adaptado de (MALTONI et al., 2009).	38
Figura 2.12 – 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).	39
Figura 2.13 – Processo de fabricação de <i>spoof</i> . (a) Fotografia do molde obtido de forma consensual com massa de modelar. (b) <i>Spoof</i> fabricado de látex. Adaptado de (YAMBAY et al., 2012).	40
Figura 2.14 – Processo de criação de um <i>spoof</i> de impressão digital pelo modo não cooperativo. Adaptado de (GHIANI et al., 2013).	41
Figura 3.1 – Ilustração da extração do padrão LBP (JIA et al., 2014).	44
Figura 3.2 – Conjuntos de vizinhanças circulares simétricas (MÄENPÄÄ; PIETIKÄINEN, 2003).	45
Figura 3.3 – Cálculo do MSLBP2 de uma matriz 9x9 . (a) Matriz 9x9 , (b) Média das regiões 3x3 da matriz original, (c) Cálculo do MSLBP2.	46
Figura 3.4 – Distribuição ótima dos raios do padrão MSLBP1 com respeito à redução de redundância da informação capturada pelo padrão. Fonte: (MÄENPÄÄ; PIETIKÄINEN, 2003).	47
Figura 3.5 – Análise dos histogramas dos padrões LBP e MSLBP1 extraídos de uma impressão digital verdadeira e de uma impressão digital falsa. Adaptado de (JIA et al., 2014).	49
Figura 3.6 - Cálculo do mapeamento relativo do pixel central. (a) Vizinhança 3x3 do pixel central g2,2 , (b) Função de mapeamento, (c) Matriz dos mapeamentos realizados na vizinhança do pixel central, (d) Matriz de pesos, (e) Mapeamento relativo à vizinhança de g2,2 .	52
Figura 3.7 – Função degrau de Heaviside gerada pelo MATLAB.	54
Figura 3.8 – Função sigmoide gerada pelo MATLAB.	54
Figura 4.1 - Amostras de imagens usadas na LivDet 2009. Em (a) é apresentada a imagem de um dedo verdadeiro, obtida com um leitor biométrico. As demais imagens, (b), (c)	

e (d) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base..... 62

Figura 4.2 - Amostras de imagens usadas na LivDet 2011. Em (a), (b) e (c) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base. 64

Figura 4.3 - Amostras de imagens usadas na LivDet 2013. Em (a) e (b) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (c), (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base. 66

Figura 4.4 - Amostras de imagens usadas na LivDet 2015. Em (a), (b) e (c) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base. 68

Figura 5.1 – *Scanner L Guardian R2 da crossmatch*. 78

LISTA DE TABELAS

Tabela 4.1 Quantidade de imagens por categoria.....	59
Tabela 4.2 - Características da base de dados LivDet 2009	61
Tabela 4.3 - Características da base de dados LivDet 2011	63
Tabela 4.4 - Características da base de dados LivDet 2013	65
Tabela 4.5 – Resultados obtidos nas bases da LivDet 2009	70
Tabela 4.6 – Resultados obtidos nas bases da LivDet 2011	71
Tabela 4.7 – Comparação dos resultados obtidos nas bases da LivDet 2013	73
Tabela 4.8 – Acurácia dos resultados obtidos nas bases da LivDet 2013	73
Tabela 4.9 – Comparação dos resultados obtidos nas bases da LivDet 2015	74

LISTA DE ABREVIATURAS E SIGLAS

PIN	Número de Identificação Pessoal (<i>Personal Identification Number</i>)
LivDet	<i>Liveness Detection Competition</i>
SVM	Máquina de Vetor de Suporte (<i>Support Vector Machine</i>)
MLP	<i>Perceptron</i> Multicamada (<i>Multilayer Perceptron</i>)
LDA	Análise Linear Discriminante (<i>Linear Discriminant Analysis</i>)
WLD	Descritor Local de Weber (<i>Weber Local Descriptor</i>)
LBP	Padrão Local Binário (<i>Local Binary Pattern</i>)
LPQ	Quantização Local em Fase (<i>Local Phase Quantization</i>)
MSLBP	Padrão Local Binário Multiescala (<i>Multi-scale Local Binary Pattern</i>)
LMP	Padrão Mapeado Localmente (<i>Local Mapped Pattern</i>)
MSLMP	Padrão Mapeado Localmente em Multiescala (<i>Multi-scale Local Mapped Pattern</i>)
FBI	<i>Federal Bureau Investigation</i>
FTIR	<i>Frustrated Total Internal Reflection</i>
CCD	<i>Charge-coupled device</i>
CMOS	<i>Complementary metal-oxide semiconductor</i>
AFIS	<i>Automatic Fingerprint Identification System</i>
KNN	<i>k</i> vizinhos mais próximos (<i>k Nearest Neighbor</i>)
FAR	Taxa de Falsos Positivos (<i>False Accept Rate</i>)
FRR	Taxa de Falsos Negativos (<i>False Reject Rate</i>),
ACE	Média dos Erros de Classificação (<i>Average Classification Error</i>)
Acc	Acurácia (<i>Accuracy</i>)
SSCA	Análise da Aspereza de Superfície (<i>Spatial surface coarseness analysis</i>)
HIG	Histogramas de Gradientes Invariantes (<i>Histograms of Invariant Gradients</i>)

SUMÁRIO

CAPÍTULO 1	16
1 INTRODUÇÃO	16
1.1 Contextualização.....	16
1.2 Motivação	18
1.3 Técnicas gerais de detecção de impressões digitais fraudulentas	19
1.4 Objetivos	22
1.5 Organização do trabalho	23
CAPÍTULO 2	25
2 CONCEITOS DE DACTILOSCOPIA.....	25
2.1 Introdução.....	26
2.2 Pontos singulares e definições em impressões digitais.....	29
2.3 Pontos Característicos de Impressões Digitais	31
2.4 Captura e reconhecimento de impressões digitais.....	32
2.5 Fraudes em Sistemas Biométricos.....	37
2.5.1 Tipos de fraudes em sistemas biométricos.....	37
2.5.2 Métodos de falsificação de impressões digitais	39
2.6 Considerações Finais	41
CAPÍTULO 3	43
3 TÉCNICA PROPOSTA	43
3.1 Considerações iniciais.....	43
3.2 Multi-Scale Local Binary Pattern (MSLBP).....	43
3.2.1 Abordagem Monoescalar	44
3.2.2 Abordagem Multiescalar	44
3.2.3 Extração de características	48
3.3 Local Mapped Pattern (LMP)	51
3.4 Multi-Scale Local Mapped Pattern (MSLMP)	53
3.4.1 Algoritmo da técnica proposta	55
3.5 Metodologia aplicada	57
3.6 Considerações finais.....	57
CAPÍTULO 4	58

4	RESULTADOS E DISCUSSÕES	58
4.1	<i>Medidas de desempenho</i>	58
4.1.1	<i>False Accept Rate (FAR)</i>	59
4.1.2	<i>False Reject Rate (FRR)</i>	59
4.1.3	<i>Average Classification Error (ACE)</i>	60
4.1.4	<i>Acurácia (Acc)</i>	60
4.2	<i>Bases de Dados</i>	60
4.2.1	<i>LivDet2009</i>	61
4.2.2	<i>LivDet2011</i>	63
4.2.3	<i>LivDet2013</i>	65
4.2.4	<i>LivDet2015</i>	67
4.3	<i>Resultados</i>	69
4.3.1	<i>LivDet 2009</i>	69
4.3.2	<i>LivDet 2011</i>	71
4.3.3	<i>LivDet 2013</i>	72
4.3.4	<i>LivDet 2015</i>	74
4.4	<i>Considerações Finais</i>	75
	CAPÍTULO 5	76
	CONCLUSÕES	76
5.1	<i>Contribuições</i>	77
5.2	<i>Trabalhos Futuros</i>	77
	REFERÊNCIAS	79
	APÊNDICE A*	83
	PROGRAMAÇÃO NO MATLAB	83
A.1	<i>Rotina para o cálculo do LMP</i>	83
A.2	<i>Rotina para a construção da matriz de características de uma base de dados</i>	84
A.3	<i>Rotina responsável por normalizar a matriz de características</i>	85
A.4	<i>Rotina responsável por definir de qual base de dados será extraído o padrão MSLMP</i>	86
A.5	<i>Rotina responsável por treinar e classificar bases de dados</i>	86
A.6	<i>Rotina que gera relatório da classificação obtida</i>	87

Capítulo 1

INTRODUÇÃO

1.1 Contextualização

Métodos de autenticação biométrica apresentam várias vantagens em relação aos meios tradicionais de autenticação. Os meios tradicionais são baseados em informações secretas conhecidas pelo usuário (*Personal Identification Number* (PIN), senha, etc) ou algo que se possui (chaves, cartões, etc) (AL-AJLAN, 2013). Portanto esses meios não possibilitam a distinção entre o usuário autêntico e um impostor, pois basta que o impostor tenha posse de um objeto ou informação que lhe garanta esse acesso para que ele se passe pelo usuário autêntico. Como os métodos tradicionais possuem vulnerabilidades, surgiu a área da biometria, que se refere 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 (MALTONI et al., 2009). Na Figura 1.1 são apresentados alguns exemplos de utilização de métodos tradicionais e biométricos de identificação.

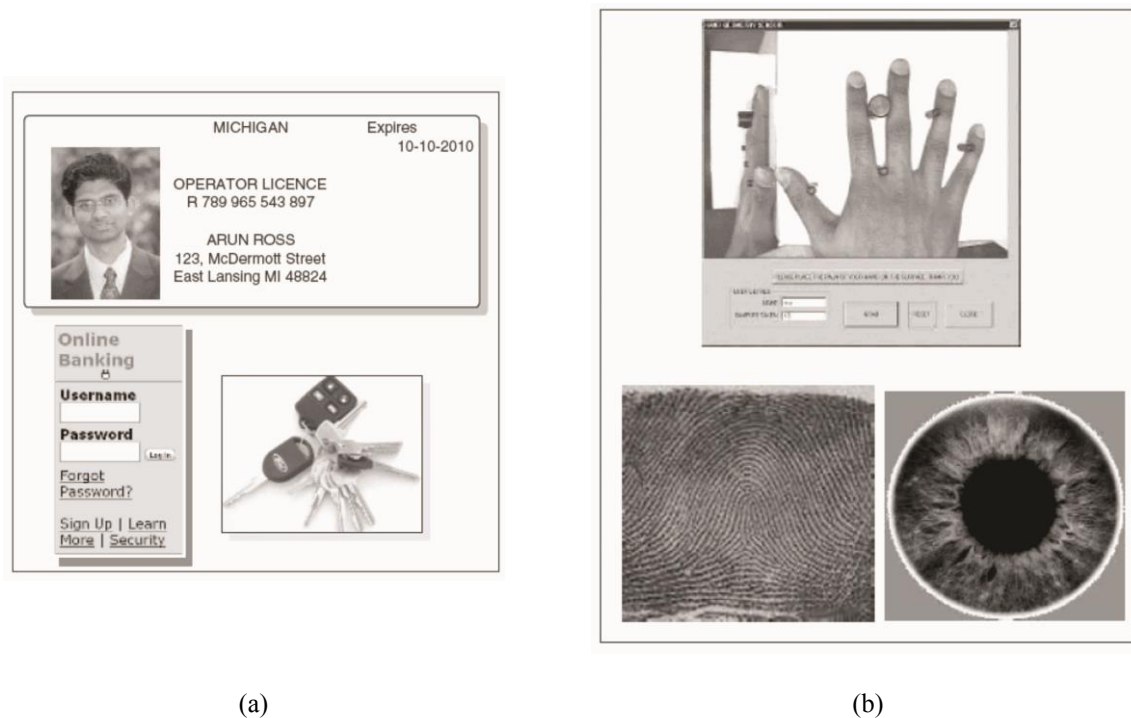


Figura 1.1 – Esquema de Autenticação. (a) Esquema tradicional utilizando Cartão de Identificação, senhas e chaves para validar o indivíduo e ter certeza que os recursos do sistema estão sendo acessados por um indivíduo legítimo. (b) Identificação com uso da biometria. Fonte: (JAIN; FLYNN; ROSS, 2007).

Em muitas aplicações, um alto nível de segurança é proporcionado por diferentes dispositivos biométricos. Em particular, os leitores de impressão digital são os mais adotados para identificação de indivíduos. Impressões digitais são muito exploradas para identificação biométrica, principalmente por sua capacidade de distinguir um indivíduo. As características de uma impressão digital de um indivíduo são únicas mesmo em gêmeos idênticos, como é citado em (KRISHAN; KANCHAN; BUMBRAH, 2012). Além disso, esse tipo de peculiaridade já é estudada há muito tempo, sendo uma abordagem bastante madura. Nenhum outro tipo de sistema biométrico foi tão bem testado no mundo real como os sistemas de impressões digitais (SOUSEDIK; BUSCH, 2014). Dentre as principais aplicações que utilizam impressões digitais pode-se citar a identificação de eleitores brasileiros por meio de urnas eletrônicas, 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.

Embora a autenticação biométrica garanta maior segurança, esses sistemas podem ser comprometidos por dados biométricos falsos. É possível burlar sua segurança pela apresentação de dedos sintéticos a um leitor de impressões digitais, como é demonstrado nos trabalhos de GALBALLY-HERRERO et al. (2006) e HOSHINO et al. (2002). Esse tipo de ataque ocorre, geralmente, quando alguém quer obter privilégios de uma pessoa autorizada (MARASCO; SANSONE, 2012) ou existe a intenção de se falsificar álibis. Inclusive, como pode ser visto nas reportagens de PEIXOTO; LOURENÇO, (2013) e de PAES (2013), a falsificação de impressões digitais (Figura 1.2) já atingiu o Brasil e é um problema que necessita urgentemente de solução.



Figura 1.2– Dedos de silicone seriam utilizados por médicos e enfermeiros para fraudar ponto eletrônico. Fonte: (PEIXOTO; LOURENÇO, 2013).

1.2 Motivação

Com o avanço das pesquisas que envolvem o reconhecimento automático de impressões digitais, a investigação de possíveis ataques que podem ocorrer em sistemas de reconhecimento biométricos se torna cada vez mais necessária. A detecção de impressões digitais sintéticas ou sua denominação em inglês, *spoof detection*, vem sendo estudada por muitos pesquisadores, buscando-se novas técnicas que garantam maior segurança aos sistemas de detecção de fraudes. Pode-se dividir as técnicas para a detecção de impressões digitais fraudulentas em duas categorias: baseadas em *software* e baseadas em *hardware* (MARASCO; SANSONE, 2012).

As técnicas baseadas em *hardware* utilizam algum dispositivo físico adicional acoplado ao leitor biométrico. Esse dispositivo é responsável por identificar características que fazem parte de um dedo humano, como: pressão sanguínea, odor da pele, temperatura,

entre outros. Por outro lado, as técnicas baseadas em *software* dispensam a adição de componentes adicionais ao leitor biométrico. A distinção entre uma impressão digital de um dedo vivo (legítimo) e uma impressão digital de um dedo falso é feita usando apenas as imagens capturadas pelo sensor (MARASCO; SANSONE, 2012). Um sistema de reconhecimento de impressões digitais falsas baseado em *software* possui a vantagem de ter menor custo financeiro visto que não é necessário a utilização de *hardware* adicional, além de ser menos invasivo por não necessitar que o usuário utilize nenhum outro equipamento além do leitor biométrico. Por isso, diversas técnicas têm sido propostas com soluções baseadas apenas em *software* para detecção de impressões digitais fraudulentas (TAN; SCHUCKERS, 2010; GALBALLY et al., 2012; MARASCO; SANSONE, 2012; PEREIRA et al., 2013; JIA et al., 2013; JIA et al., 2014; GRAGNANIELLO et al., 2014).

A abordagem baseada em *software*, segundo SOUSEDIK; BUSCH (2014), possui ainda duas categorias: estática e dinâmica. Na abordagem estática, uma única imagem é utilizada para extrair as informações necessárias ao reconhecimento de uma impressão digital falsa (MALTONI et al., 2009). Por outro lado, a abordagem dinâmica usa um conjunto de quadros (*frames*) extraídos em determinados intervalos de tempo, isto é, o usuário deverá manter o dedo pressionado sobre o sensor para que a extração dos padrões presentes na impressão digital seja feita mais de uma vez.

1.3 Técnicas gerais de detecção de impressões digitais fraudulentas

Dada a proximidade do tema e da data da confecção deste trabalho com o trabalho de SILVA (2014), os estudos aqui discutidos sobre o atual estado da arte do problema em questão foram baseados no referido trabalho. Desta forma, a disposição dos tópicos, assim como o texto contido em alguns parágrafos desta seção foram extraídos da dissertação de SILVA (2014).

Diversas técnicas têm sido propostas a fim de detectar impressões digitais falsas. Como foram citadas na seção anterior deste capítulo, as técnicas apresentadas no estado da arte podem ser divididas em soluções: baseadas em *software* e baseadas em *hardware*. As soluções baseadas em *software* não necessitam de nenhum *hardware* adicional para que seja feito o reconhecimento do indivíduo. Já nos métodos baseados em *hardware*, algum

equipamento é adicionado ao sensor para detectar características adicionais como: pressão sanguínea, odor, temperatura, entre outros. Soluções baseadas em *software* têm a vantagem de serem menos custosas financeiramente e menos invasivas, o que as tornam mais atrativas para uma aplicação prática, como pode ser visto no trabalho de MARASCO; SANSONE (2012).

Os métodos estáticos, como dito anteriormente, usam apenas uma imagem de impressão digital. Esses métodos analisam várias especificidades de imagens de dedos verdadeiros e dedos falsos que são causadas por diferentes características. Com base nisso, AL-AJLAN (2013) faz uma divisão mais detalhada com respeito a esses métodos, como pode ser observado na Figura 1.3.

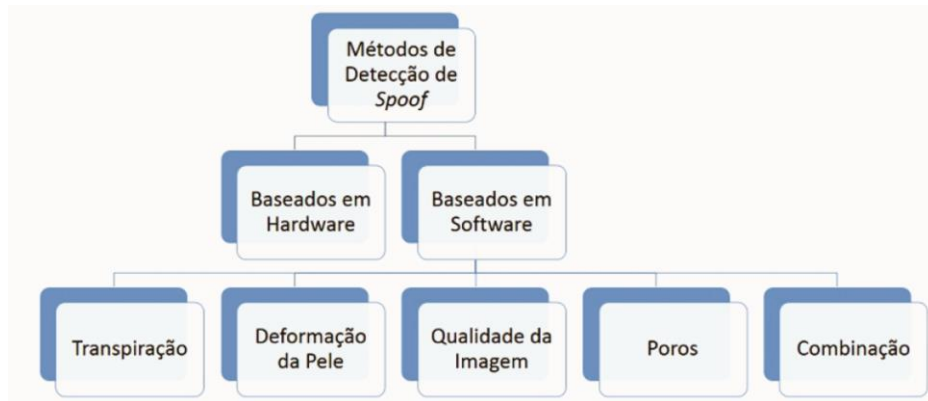


Figura 1.3 – Representação do estado da arte das pesquisas de métodos de detecção de *spoof*. Adaptado de (AL-AJLAN, 2013).

A detecção de impressões digitais fraudulentas através da abordagem estática é, de forma geral, realizada em três etapas, a saber:

- (1) extração de características: um vetor $v_f \in \mathbb{R}^n$ é associado à imagem f , no qual o valor de sua i -ésima dimensão armazena o valor da característica avaliada pela função $\lambda_i : F \rightarrow \mathbb{R}$, $i \in \{1, 2, \dots, n\}$, na qual $n \in \mathbb{N}$ é o número total de características utilizadas pela técnica e F é a base de dados que contém as imagens f . Desta forma, o vetor de características que representa a imagem f é dado por $v_f = (\lambda_1(f), \lambda_2(f), \dots, \lambda_n(f))$.
- (2) seleção de características: um novo vetor v_f' é criado eliminando algumas dimensões de v_f que possuem menor poder de discriminação entre exemplares autênticos e forjados. O objetivo é determinar o subconjunto ótimo de dimensões do vetor de características a ser analisado para cada uma das bases de dados do

problema. Embora esta etapa seja omitida em algumas soluções, vários trabalhos na literatura fazem uso dela (GALBALLY; MARCEL; FIERREZ, (2014); GRAGNANIELLO et al., (2014)).

- (3) Classificação: cada vetor de teste v_f' é avaliado por um classificador binário para o qual diversas instâncias, de amostras autênticas e falsas, foram previamente apresentadas durante um ciclo de treinamento.

Geralmente, as técnicas responsáveis pela classificação de impressões digitais, citadas no item (3), fazem uso de métodos de aprendizagem supervisionada.

MARASCO; SANSONE (2012) propõem uma técnica baseada em características morfológicas e de transpiração e combina várias características como: distância entre poros, razão de intensidades de níveis de cinza, rugosidade da superfície e outras características do estado da arte. Seus experimentos foram realizados na base de dados *Liveness Detection Competition 2009* (LivDet 2009). Para o treinamento e classificação os autores utilizam a combinação de três classificadores: *Support Vector Machine* (SVM), rede neural *Multilayer Perceptron* (MLP) e *OneR*.

MOON et al. (2006) defendem que dedos falsos, confeccionados a partir de materiais sintéticos, possuem macromoléculas que tendem a se aglomerar e, por essa razão, as imagens de impressões digitais falsas são mais “granulares” em relação às imagens de dedos vivos. O método utilizado por (MOON et al., 2006) consiste em um procedimento baseado na transformada *wavelet* para obter uma imagem sem ruído e então o ruído é calculado através da subtração da imagem original pela imagem suavizada. O desvio padrão do ruído é usado para distinguir uma impressão digital falsa de uma verdadeira (SOUSEDIK; BUSCH, 2014).

PEREIRA et al. (2013) apresentam uma nova técnica baseada na técnica de (MOON et al., 2006). Nesta técnica, é utilizada a rugosidade da superfície a imagens de baixa resolução, obtendo precisão 70,09% maior que a técnica original aplicada à base *Liveness Detection Competition 2011* (LivDet 2011). Em seguida, faz-se uso de um classificador SVM para o treinamento e classificação.

GALBALLY et al. (2012) propõem um método de detecção baseado em múltiplas características. Estas características são baseadas na continuidade e suavidade do fluxo das cristas papilares. Seus experimentos são testados em uma base de dados com 10.500 imagens de dedos vivos e falsos. Essa técnica consegue 90% de classificação correta nas amostras da

base de dados utilizada usando a Análise Linear Discriminante (*Linear Discriminant Analysis* (LDA)) como classificador.

GRAGNANIELLO et al. (2013) propõem uma técnica baseada no micropadrão *Weber Local Descriptor* (WLD). A técnica calcula dois coeficientes: *differential excitation* e orientação de uma imagem, em que cada uma dessas características é extraída de cada pixel da imagem e depois o histograma conjunto dessas duas características é usado para criar um vetor de características que serve para discriminar impressões digitais de dedos vivos de impressões de dedos falsos. Esta abordagem foi avaliada nas bases de dados LivDet 2009 e LivDet 2011 usando um classificador SVM. Os autores ainda combinam a técnica com o micropadrão *Local Binary Patterns* (LBP) de OJALA; PIETIKÄINEN; HARWOOD (1996) e com o micropadrão *Local Phase Quantization* (LPQ) de OJANSIVU; RAHTU; HEIKKILA (2008) obtendo resultados que superam a técnica original.

Métodos dinâmicos usam uma série de imagens adquiridas em intervalos diferentes de tempo. Além de se basear em algumas características inerentes a cada imagem, também leva em consideração a diferença entre as imagens que foram capturadas nos diferentes espaços de tempo. SOUSEDIK; BUSCH (2014) apresentam as seguintes características que podem ser usadas nesse método: distorção da pele e transpiração. Foge ao escopo desse trabalho apresentar maiores detalhes a respeito do método dinâmico, pois a técnica aqui empregada trata de uma técnica estática baseada apenas em *software*.

1.4 Objetivos

Esta dissertação propõe uma técnica de reconhecimento de impressões digitais fraudulentas tendo como base a extração e análise do padrão denominado Padrão Mapeado Localmente em Multiescala (*Multi-Scale Local Mapped Pattern* (MSLMP)). Esta técnica é baseada em *software* e usa uma única imagem de impressão digital para extração de características, sendo desta forma classificada como estática.

O MSLMP é uma versão estendida na forma multiescalar do padrão *Local Mapped Pattern* (LMP) de (FERRAZ; JUNIOR; GONZAGA, 2014) o qual consiste em realizar o mapeamento local do padrão representado pela vizinhança 3x3 de um pixel, como pode ser

observado na Figura 1.4. O padrão MSLMP, proposto neste trabalho, considera vizinhanças de tamanho variável neste cálculo.

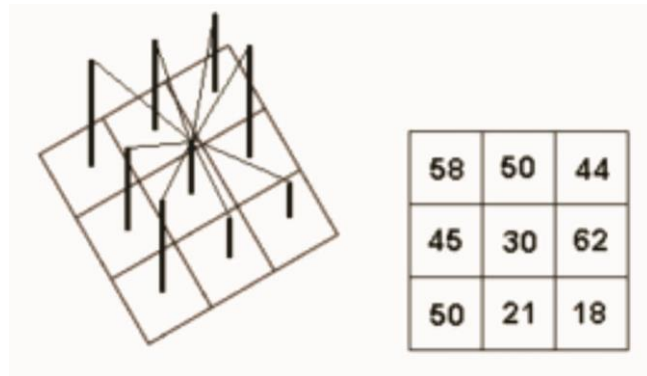


Figura 1.4 – Diferenças de níveis de cinza como um padrão local. Fonte: (FERRAZ; JUNIOR; GONZAGA, 2014).

O objetivo do trabalho consiste em apresentar e implementar o algoritmo de classificação de impressões digitais fraudulentas baseado no padrão MSLMP e avaliar sua eficácia diante de algumas bases de dados de impressões digitais disponíveis na literatura e comparar os resultados obtidos com os melhores trabalhos disponibilizados no estado da arte na literatura científica especializada.

1.5 Organização do trabalho

Além deste capítulo introdutório, no qual foram apresentados os objetivos e motivações para este trabalho, esta dissertação se divide em mais quatro capítulos.

No Capítulo 2 introduz-se os principais termos e conceitos de Biometria abordados neste trabalho, trazendo também algumas informações sobre sistemas biométricos. Além disso, também são apresentados os principais ataques que os sistemas biométricos podem sofrer e os ataques específicos para sistemas baseados em impressões digitais.

No Capítulo 3 aborda-se padrões utilizados para detecção de impressões digitais falsas. Também é descrita a técnica proposta neste trabalho e, finalmente, formula-se o algoritmo responsável por classificar impressões digitais como verdadeiras ou falsas.

No Capítulo 4 são apresentados os resultados dos experimentos que foram realizados sobre as bases LivDet2009, LivDet2011, LivDet2013 e LivDet2015, e é feita uma comparação com os resultados presentes na literatura.

No Capítulo 5 reúnem-se as considerações finais e as expectativas do presente trabalho.

Por fim, encontram-se no Apêndice A* algumas rotinas implementadas no trabalho que foram consideradas mais específicas deste problema. O ambiente de desenvolvimento utilizado para a construção dos roteiros de programação foi o MATLAB 2013®.

Capítulo 2

CONCEITOS DE DACTILOSCOPIA

Estudos e aplicações de impressões digitais estiveram sempre presentes na história da humanidade. Artefatos arqueológicos encontrados no nordeste da China apresentam peças de barro datadas de mais de 6000 anos apresentando afrescos com características de impressões digitais. Sabe-se que, em 300 AC, impressões digitais eram utilizadas como prova de crime na China e que “apenas” em 702 DC passaram a ser utilizadas no Japão para o mesmo fim (KRISHAN; KANCHAN; BUMBRAH, 2012).

O termo dactiloscopia vem do grego *daktylos* que significa dedos e *skopein* que significa examinar. Este termo foi proposto pelo Doutor Francisco Latzina para referir-se a sistemas de verificação de impressões digitais (KEHDY, 1968). Atualmente, com o crescente avanço e desenvolvimento das tecnologias ligadas ao processamento digital de imagens, existe o interesse em se aplicar os conceitos relativos à dactiloscopia para a criação de sistemas automáticos de reconhecimento de impressões digitais. Esse capítulo tem como objetivo a apresentação dos conceitos relativos à composição de uma impressão digital e algumas de suas principais características.

SILVA (2014) e CASTRO (2008) abordam muito claramente em suas respectivas dissertações os tópicos presentes neste capítulo. Desta forma, tendo em vista que este é um assunto muito conhecido no estado da arte, foram utilizadas em alguns parágrafos seções de textos presentes nos trabalhos de SILVA (2014) e de CASTRO (2008).

2.1 Introdução

Atualmente, atividades relacionadas com a identificação pessoal, como atividades bancárias, controle de acesso, atividades jurídicas, etc, exigem que os processos que dependem de recursos ligados à identificação biométrica sejam rápidos, eficientes e seguros para a confirmação de identidade (USMANI et al., 2013). Para isto, sistemas biométricos de identificação automática têm sido utilizados visando caracterizar os indivíduos segundo características biológicas específicas. Segundo (MALTONI et al., 2009) um sistema de identificação biométrica que seja considerado eficiente deve levar em consideração as seguintes características:

- universalidade: cada indivíduo pode ser classificado por um conjunto de características;
- unicidade: indica que dois indivíduos não possuem as mesmas características;
- permanência: as características não podem ser modificadas naturalmente;
- critério quantitativo: essas características podem ser medidas de forma quantitativa.

MALTONI et al. (2009) ainda apresentam outras questões que devem ser levadas em consideração em um sistema particular ao selecionar uma característica:

- desempenho: precisão do reconhecimento, velocidade, necessidade de recursos e robustez;
- aceitabilidade: disponibilidade dos usuários aceitarem o identificador biométrico em seu dia a dia;
- contornabilidade: possibilidade de um sistema biométrico poder ser contornado por um método fraudulento.

Atualmente diversos meios de identificação biométrica têm sido usados e estudados. Alguns dos principais são:

- íris: órgão localizado no olho de um ser humano que é formado por volta do oitavo mês de gestação. Apresenta textura variada para cada pessoa (DAUGMAN, 1996). A captura da imagem da íris é feita com a cooperação do indivíduo, pois é necessário que ele se encontre a uma determinada distância

da câmera e que o ponto central da imagem foque na íris (MALTONI et al., 2009).

- face: um dos meios de identificação mais usados pelos seres humanos. Diariamente, indivíduos reconhecem a face de seus familiares e amigos identificando-os entre outras pessoas nunca antes vistas. O uso de um computador para reconhecer um indivíduo por sua face não é invasivo, visto que as imagens de uma pessoa não requerem necessariamente que esta interaja com a câmera ou se posicione muito próximo dela.
- geometria da mão ou dos dedos: algumas características das mãos dos seres humanos são relativamente invariantes e peculiares, é o caso do tamanho dos dedos, embora não tenham um grande poder de distinção. Um dos atrativos ao uso desse tipo de peculiaridade é que a criação dos padrões (*templates*) que a representam possui tamanho reduzido. Os sistemas biométricos baseados na geometria dos dedos, em vez de toda a mão, podem ser preferidos, pois seus *templates* possuem tamanho ainda menor (MALTONI et al., 2009).
- veias dos dedos ou da mão: um raio infravermelho é usado para capturar imagens da estrutura das veias das mãos ou dedos de um indivíduo que são usadas para criação de um padrão que representa essa peculiaridade (MALTONI et al., 2009).
- voz: constitui uma peculiaridade aceitável da perspectiva do usuário. Uma das motivações para o uso da voz como peculiaridade é dada pelas diferenças existentes nas cordas vocais, no trato vocal e em todo o aparelho fonador dos indivíduos (ASHBOURN, 2002).
- assinatura: uma vantagem dessa peculiaridade é que ela é percebida como uma ação natural e familiar. A assinatura traz informações acerca não somente da aparência mas também da dinâmica que envolve a pressão exercida com a caneta na superfície em que se escreve, o quão rápido se escreve e até onde cruza-se a letra "T" ao escrevê-la (ASHBOURN, 2002).

Uma impressão digital é uma característica única de cada indivíduo que possui como uma grande vantagem a permanência de suas características durante os anos (PANKANTI; MEMBER; PRABHAKAR, 2002), desta forma, é razoável que essa propriedade permita tornar a impressão digital bastante atrativa para o uso em identificações biométricas. Como todas as pessoas possuem impressões digitais, logo esse é um critério universal, salvo

algumas exceções de pessoas que perderam os dedos, ou removeram suas digitais (casos não naturais). Impressões digitais são formadas no período da gestação (aos quatro meses) e acompanham o indivíduo durante todo seu ciclo de vida (KRISHAN; KANCHAN; BUMBRAH, 2012). Algumas pesquisas que dizem respeito à dactiloscopia sugerem como realizar a quantificação desses parâmetros biométricos, muitas dessas pesquisas indicam que a localização de 12 pontos característicos ou minúcias são suficientes para confirmar a identidade de um indivíduo (XIAO; RAAFAT, 1991), (ELECCION, 1973).

As expressões existentes na pele dos dedos que formam as impressões digitais são chamadas de linhas dactilares e podem ser subdivididas em cristas e vales. As cristas são as regiões mais acentuadas e que geralmente são representadas pelas linhas mais escuras nas imagens de impressões digitais capturadas por sensores, enquanto que os vales são as regiões que separam uma crista da outra. Na Figura 2.1 a seguir tem-se um exemplo de impressão digital na qual pode-se observar o comportamento das cristas ao longo da imagem, regiões com cristas paralelas, convergências entre cristas e algumas apresentando formas específicas.

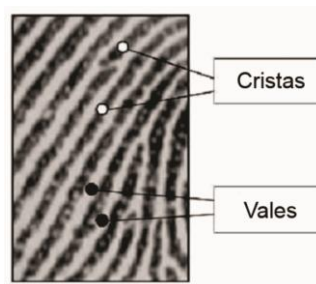


Figura 2.1 – Exemplo de impressão digital. Adaptado de (JAIN; FLYNN; ROSS, 2007).

Dois critérios costumam ser utilizados para classificar impressões digitais. O primeiro critério faz uso de uma forma global para avaliar o comportamento das linhas dactilares da impressão, visando classificar a que grupo esta pertence. O segundo critério permite analisar a identidade de um indivíduo através de minúcias presentes na imagem, que ocorrem quando há uma convergência entre cristas ou quando há a terminação abrupta desta (JAIN; HONG; BOLLE, 1997). Esses critérios encontram-se melhor detalhados na próxima seção.

2.2 Pontos singulares e definições em impressões digitais

Francis Galton realizou um estudo sobre as características das impressões digitais e, em 1888, lançou as bases científicas para o estudo da dactiloscopia visando estabelecer um sistema de identificação (KRISHAN; KANCHAN; BUMBRAH, 2012). Este pesquisador foi o primeiro a observar pontos característicos na formação das linhas dactilares da pele, onde as cristas sofrem pequenas modificações em seu comportamento natural, convergindo sobre cristas próximas ou terminando de maneira abrupta, como pode ser visto em (GALTON, 1892).

Edward Henry, em 1905, foi o primeiro a realizar a classificação das impressões digitais baseado na distribuição das cristas na imagem, os chamados detalhes globais, e definiu os pontos singulares como as regiões onde as linhas dactilares apresentam uma estrutura no formato de delta ou em formato circular que dá origem ao núcleo (HENRY, 1905).

Atualmente, considera-se que a impressão digital pode ser composta por cristas finais ou terminações, cristas bifurcadas, cruzamento, esporas e ilhas, dependendo da forma que a minúcia se apresente (MALTONI et al., 2009). Os pontos singulares são as primeiras características observadas ao se realizar uma análise em uma impressão digital. O primeiro ponto singular que se pode destacar é o núcleo, que corresponde ao ponto central de uma impressão digital, envolto por linhas dactilares. Dependendo da forma como as cristas estão dispostas na região central, pode-se classificar o núcleo como Verticilo quando as linhas circundarem o elemento central ou Laço quando essas contornarem o ponto central. Existem ainda impressões digitais que não possuem ponto central definido em função da distribuição assumida por suas cristas. Para esses casos, o núcleo da imagem poderá ser encontrado utilizando a região interna que possua cristas com maior curvatura (HENRY, 1905).

Outro elemento singular é o Delta, destacado na Figura 2.2, com cristas salientes que podem ser formadas por dois processos: a bifurcação de uma linha simples ou a brusca convergência de duas linhas paralelas. Esta estrutura determina um importante papel na classificação de impressões digitais, pois a quantidade de deltas indica a classe dessa imagem. Deltas tendem a representar o ponto de divergência das linhas dactilares mais internas que envolvem a região nuclear (MALTONI et al., 2009).



Figura 2.2 – Exemplo de singularidade Delta. Impressão Digital de (GHIANI et al., 2013) .

A Figura 2.3 apresenta exemplos das cinco classes propostas por Henry no trabalho (HENRY, 1905), com as características definidas a seguir:

- (a) **verticilo**: apresenta dois deltas: um a direita e outro a esquerda do núcleo. As cristas internas a esses deltas apresentam um padrão concêntrico, espiralado, oval ou mesmo sinuoso com um centro bem definido.
- (b) **presilha interna**: as linhas dactilares se formam à esquerda do observador, curvam-se no centro e tendem a retornar para o mesmo lado de formação. Apresentam um delta à direita da região nuclear.
- (c) **presilha externa**: as linhas dactilares se formam à direita do observador, curvando-se no centro com tendência a retornar para o mesmo local de formação. Apresenta um delta à esquerda da região nuclear.
- (d) **arco plano**: as linhas dactilares formam-se de um lado e tendem a sair do outro lado da digital. Mostram forma abaulada e não apresentam deltas.
- (e) **arco angular**: linhas semelhantes aos Arcos Planos, mas apresentando uma elevação acentuada no centro da imagem no formato de uma tenda.

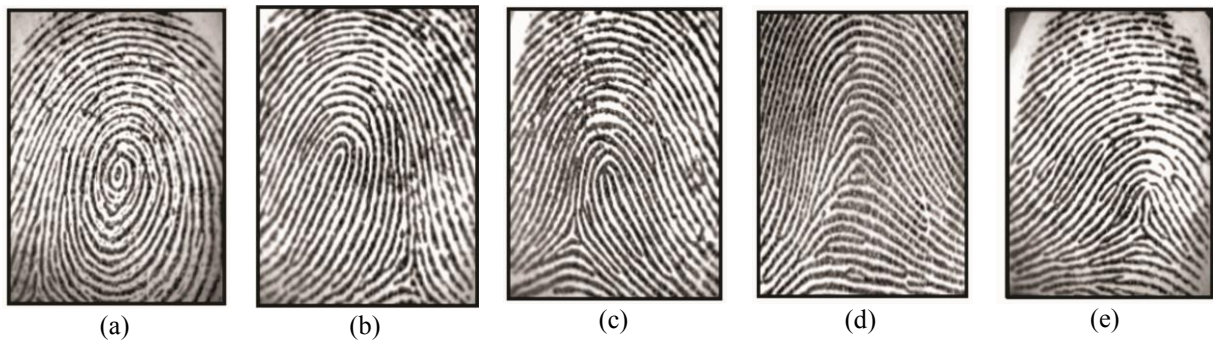


Figura 2.3 – Regiões singulares de Henry. (a) Verticilo, (b) Presilha Interna, (c) Presilha Externa, (d) Arco Plano, (e) Arco Angular. Adaptado de (MALTONI et al., 2009).

2.3 Pontos Característicos de Impressões Digitais

Minúcias, também conhecidas como características de Galton, são regiões que contêm singularidades encontradas em linhas papilares, que fazem com que a crista fuja do seu arranjo natural, vindo a terminar abruptamente ou se bifurcar (GALTON, 1892).

Na Figura 2.4 tem-se alguns exemplos das características de Galton contendo sete tipos de minúcias que podem ser utilizadas para a identificação de indivíduos em um sistema biométrico. Em (a) é apresentado um exemplo de uma bifurcação obtida através da convergência de duas cristas paralelas. Em (b) tem-se o exemplo de uma crista final, ou terminação, caracterizado pela finalização abrupta de uma crista. Em (c) percebe-se um exemplo de uma minúcia composta, chamada de lago, que é formada pela união de duas bifurcações na mesma crista. Em (d) é apresentado um exemplo de cruzamento (*crossover*) onde se observa a intersecção de uma crista com uma bifurcação. A minúcia presente em (e) é conhecida como ilha, pois é representada por uma crista relativamente pequena envolta de uma depressão formada por vales. Pode ser visto em (f) o que seria um “negativo” de uma ilha, chamado de crista independente. Finalmente, em (g) pode-se ver o que é conhecido como esporo, cuja caracterização é dada por uma semi bifurcação em uma crista.

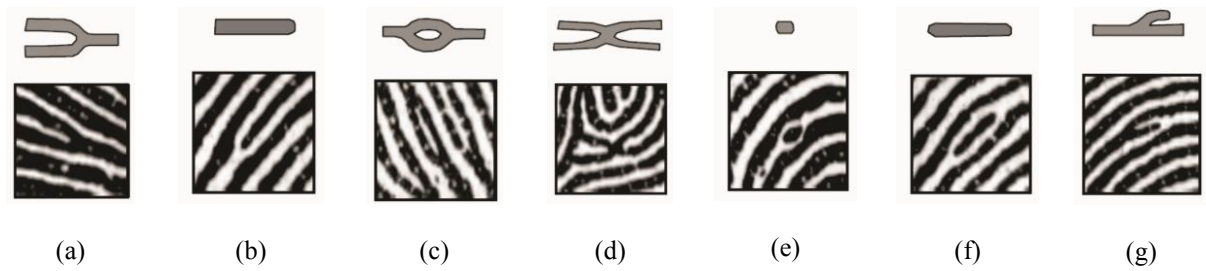


Figura 2.4 – Singularidades relativamente locais. (a) Bifurcação, (b) Terminação, (c) Lago, (d) Cruzamento, (e) Ponto, (f) Crista Independente e (g) Espora. Adaptado de (MALTONI et al., 2009).

Normalmente, encontrar os tipos de minúcias apresentadas da Figura 2.3 facilita muito o processo de pré-seleção das imagens dentro de um banco de dados, selecionando aquelas imagens que possuam a característica desejada.

Para fins criminais e visando aumentar a segurança do reconhecimento biométrico do sistema, o FBI (*Federal Bureau Investigation*) requer o casamento de, no mínimo, 20 pontos característicos entre o indivíduo comparado e o *template* em questão para a confirmação da identidade investigada (FBI: FEDERAL BUREAU OF INVESTIGATION, 1984).

2.4 Captura e reconhecimento de impressões digitais

Para a aquisição das imagens das impressões digitais podem ser utilizados diversos tipos de sensores (ópticos, capacitivos, ultrassônicos, etc). A estrutura padrão do funcionamento de um sensor responsável pela captura de impressões digitais é mostrada na Figura 2.5. 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, por exemplo, um computador.

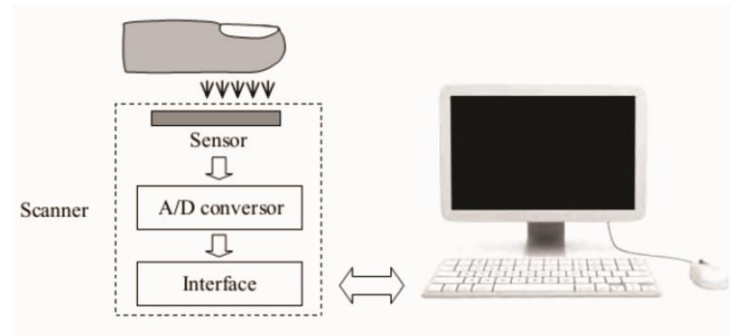
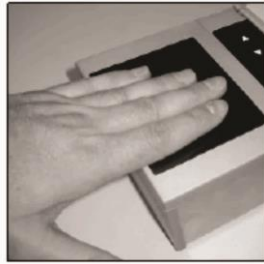


Figura 2.5 – Ilustração do funcionamento geral de um sensor de impressões digitais. Adaptado de (MALTONI et al., 2009).

Para que um sistema biométrico seja considerado seguro, seu desenvolvimento deve ser baseado em mecanismos de proteção nos sensores e requer a implementação de algum setor responsável pela criptografia no processo de comunicação do sensor com o dispositivo externo e também entre os módulos do sistema biométrico. Na seção seguinte 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. MALTONI et al. (2009) classificam os sensores de impressões digitais nas seguintes categorias:

- **multi-dedos:** mais de um dedo pode ser capturado simultaneamente conforme ilustra a Figura 2.6 (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 2.7.
- **único-dedo:** apenas um dedo é capturado por vez conforme ilustra a Figura 2.6 (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.



(a)



(b)

Figura 2.6 – 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 (MALTONI et al., 2009).



Figura 2.7 – Um exemplo de imagem com 500dpi capturada com um scanner multidedos *Papillon DS-30*, os quatro retângulos mostram a posição das quatro impressões digitais localizadas por um algoritmo de segmentação automática. Adaptado de (MALTONI et al., 2009).

Pode-se dividir as tecnologias de aquisição de impressões digitais em dois grupos. A primeira categoria é representada pelo grupo dos sensores óticos que faz uso de um sistema de fontes de luz: lentes, prismas ou fibra ótica ao longo de uma superfície fotossensível para capturar os padrões da impressão digital. Já os sensores de estado sólido representam a segunda categoria de sensores, que são geralmente de tamanho menor que os óticos, visto que o mecanismo que captura a impressão digital é integrado em um chip de silício. Os sensores de estado sólido, por possuírem tamanho reduzido, podem ser integrados em um dispositivo

portátil (SOUSEDIK; BUSCH, 2014). Dois sensores, um de cada categoria, são apresentados aqui para ilustrar melhor como essas tecnologias funcionam.

O *Frustrated Total Internal Reflection* (FTIR) usa um prisma, uma luz de LED e uma câmera CCD/CMOS (*charge-coupled device / complementary metal-oxide semiconductor*) como mostra a Figura 2.8. O dedo é colocado em contato com a superfície do prisma. As cristas da impressão digital que estão em contato com o prisma absorvem a luz enquanto que a superfície sob os vales reflete a luz para a câmera CCD/CMOS. Esse sensor dificulta a tentativa de fraudar um usuário verdadeiro pela apresentação de uma imagem 2D de uma impressão digital. No entanto, essa tecnologia tem o problema de possuir um tamanho grande devido ao tamanho do prisma. Outras tecnologias são usadas para solucionar esse problema: folhas de prismas, placa de fibra ótica, entre outras. SOUSEDIK; BUSCH (2014) fizeram um trabalho mais detalhado com respeito à engenharia dos sensores.

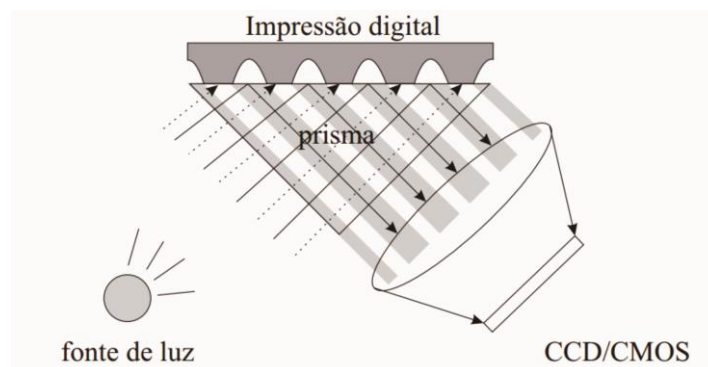


Figura 2.8 – Representação funcional de um *Frustrated Total Internal Reflection* (FTIR). Adaptado de (SOUSEDIK; BUSCH, 2014).

Diferente dos sensores óticos, os sensores de estado sólido, também conhecido por sensor capacitivo, podem ser integrados em um único *chip*, reduzindo o tamanho e o custo. Um exemplo é o sensor baseado em pressão (Figura 2.9), que é construído com base no efeito de um material piezoelétrico. Esse material produz uma pequena voltagem quando uma pressão é aplicada. Essa tecnologia usa uma grade (*grid*) de células piezoelétricas que produzem diferentes voltagens dependendo se elas estão ou não em contato com as cristas papilares da impressão digital. O padrão da impressão digital é formado baseado nas diferenças de voltagem (SOUSEDIK; BUSCH, 2014).

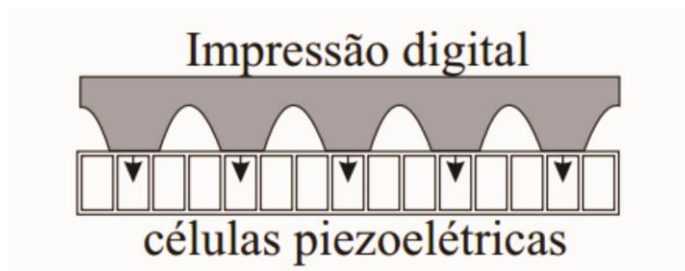


Figura 2.9 – Representação funcional de um Sensor piezoelétrico. Adaptado de (SOUSEDIK; BUSCH, 2014).

Através desses e de outros tipos de leitores, as imagens de impressões digitais são obtidas. Essas imagens podem ser armazenadas em bases de dados do governo ou outros órgãos para diferentes finalidades. Em todo caso, em algum momento, é provável que haja a necessidade de fazer a comparação (*matching*) entre uma impressão digital de um indivíduo e alguma outra que se encontra em uma base de dados. Os Sistemas Automáticos de Identificação de Impressões Digitais (*Automatic Fingerprint Identification System (AFIS)*) reduzem drasticamente o tempo necessário de comparação de impressões digitais (ASHBOURN, 2002). E são esses sistemas que tornam viável a utilização em larga escala de impressões digitais no processo de identificação de indivíduos. Esses sistemas fazem a busca e casamento (*match*) das minúcias nas impressões digitais para identificar se a pessoa que colocou seu dedo em um sensor é realmente a pessoa autorizada a usar o sistema. Os pontos singulares e característicos de uma impressão digital juntos às minúcias estudadas nas seções anteriores geralmente formam um conjunto de características muito eficiente para a realização dessas identificações. A Figura 2.10 a seguir mostra um exemplo de minúcias usadas para a comparação de impressões digitais.



Figura 2.10 – Exemplo de minúcias usadas para o *match* entre impressões digitais. (ASHBOURN, 2002).

2.5 Fraudes em 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 (MALTONI et al., 2009). 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, pois, existem vulnerabilidades que podem ser exploradas em sistemas biométricos. Estas vulnerabilidades surgem com a utilização de biometria, pois, 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 a cada dia, necessitando, assim, de um esforço contínuo em pesquisas para criar mecanismos de segurança. Segundo MALTONI et al. (2009), um modelo de segurança é baseado em o que se precisa proteger e de quem, levando em consideração os possíveis ataques já conhecidos. Desta forma, os diferentes tipos de sistema e tipos de uso é que vão definir quais são as técnicas de segurança necessárias para proteger os dados e acessos ao sistema.

No trabalho de BIGGIO et al. (2012) são apresentadas vulnerabilidades potenciais em sistemas biométricos, e alguns trabalhos, como (SCHNEIER, 1999), revelaram que não apenas os módulos do sistema podem ser atacados, mas também os canais de comunicação utilizados por eles.

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 comprometer a integridade dos dados (BIGGIO et al., 2012).

2.5.1 Tipos de fraudes em sistemas biométricos

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. A Figura 2.11 ilustra oito pontos através dos quais tais sistemas podem ser atacados, permitindo a autenticação de indivíduos

não autorizados (MALTONI et al., 2009). As principais possibilidades de fraude são as seguintes:

- (a) interceptação dos canais de comunicação indicados pelos dos números (2), (4), (6) e (8) na Figura 2.11, e substituição dos dados transmitidos;
- (b) substituição dos módulos que compõem as fases indicadas pelos dos números (3) e (5) na Figura 2.11. Isto é, um algoritmo de casamento que sempre responda positivamente, ou um módulo de extração de minúcias que sempre forneça os dados de um cliente cadastrado;
- (c) edição ou adição de *templates* biométricos contidos no módulo indicado pelo número (7) na Figura 2.11. Ou seja, o cadastramento ilegal de um novo usuário no sistema;
- (d) apresentação de uma impressão digital sintética, gerada mediante cópia da informação biométrica de um usuário cadastrado, ao sensor utilizado na fase indicada pelo número (1) na Figura 2.11.

As fraudes (a), (b) e (c), citadas anteriormente, exigem do contraventor um conhecimento técnico do sistema bastante elevado. No entanto, algumas falhas na distribuição do serviço em rede podem facilitar o crime, por exemplo, ausência de criptografia nos canais de comunicação indicados, na Figura 2.11, pelos números (2), (4), (6) e (8) ou execução das fases indicadas pelos números (3), (5) e (7) em servidores desprotegidos. De qualquer forma, a fraude (d) é igualmente perigosa e praticada com relativa facilidade, e é este tipo de fraude que o presente trabalho procura combater.

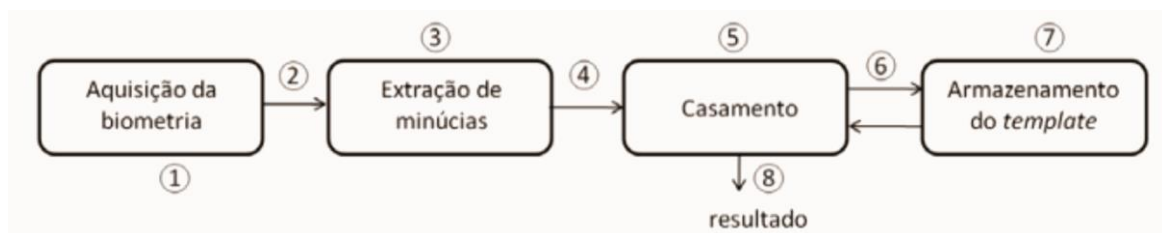


Figura 2.11 – Oito pontos através dos quais um sistema de reconhecimento de impressões digitais pode ser atacado, permitindo, assim, a autenticação de indivíduos não autorizados. Adaptado de (MALTONI et al., 2009).

2.5.2 Métodos de falsificação de impressões digitais

Apresentar uma falsa peculiaridade ao sensor é um dos tipos de ataque mais comuns a sistemas biométricos. Esse tipo de ataque é conhecido como *spoofing*. No caso de impressões digitais, este tipo de ataque pode ser realizado simplesmente apresentando uma impressão digital construída artificialmente ao sensor, ou então, utilizando um dedo desmembrado ou de um cadáver (JAIN; FLYNN; ROSS, 2007).

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 pode ser utilizada para deixar impressões digitais falsas em objetos (MALTONI et al., 2009). Trabalhos como o de MATSUMOTO et al. (2002) e o de GALBALLY-HERRERO et al. (2006) 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 2.12 é possível visualizar o molde e o *spoof* criados para os testes realizados.

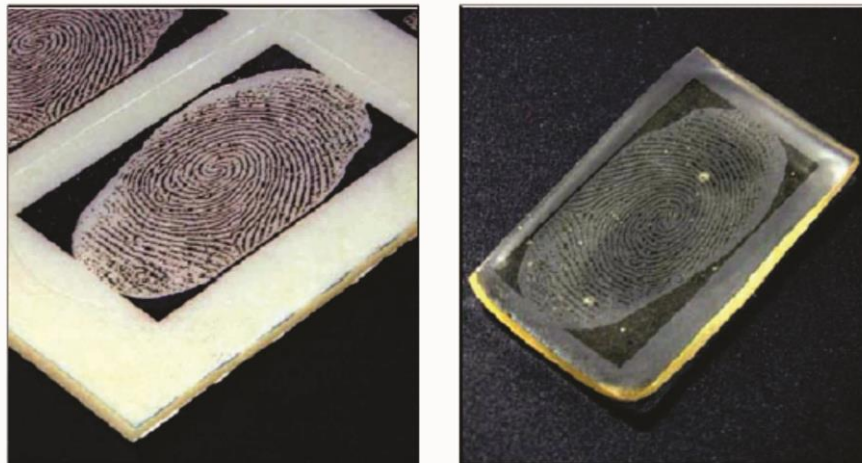


Figura 2.12 – Fotografia da aparência externa do molde e do dedo de goma. O dedo de goma foi produzido a partir de uma impressão digital latente deixada em uma placa de vidro e melhorada utilizando uma cola (MATSUMOTO et al., 2002).

Os métodos de falsificação de impressões digitais podem ser divididos em duas categorias (SOUSEDIK; BUSCH, 2014): os métodos cooperativos e o não cooperativos. No

primeiro caso, tem-se acesso ao dedo do indivíduo de forma voluntária. Por outro lado, no segundo caso, o dedo de um indivíduo não está diretamente disponível.

Nos métodos cooperativos a falsificação pode ser feita usando moldes de materiais, tais como: silicone, cera de vela, goma de algodão, entre outros. O molde precisa ser suficientemente flexível, permitindo que o dedo seja colocado nele para formar o negativo da impressão digital. Isso precisa ser feito de maneira cuidadosa, a fim de preservar os detalhes da impressão digital. Após o molde ser confeccionado a falsificação pode ser feita usando materiais que simulam o local onde se depositam, tais como: látex, silicone, gelatina e outros. Os materiais do molde e da impressão falsa não podem juntar um com o outro durante o processo (SOUSEDIK; BUSCH, 2014). A Figura 2.13 (a) mostra uma fotografia do molde confeccionado com massa de modelar e a Figura 2.13 (b) apresenta o *spoof* criado a partir do molde com látex.



(a)



(b)

Figura 2.13 – Processo de fabricação de *spoof*. (a) Fotografia do molde obtido de forma consensual com massa de modelar. (b) *Spoof* fabricado de látex. Adaptado de (YAMBAY et al., 2012).

Os métodos não cooperativos usam outros meios para confeccionar a falsificação. Impressões digitais latentes encontradas em várias superfícies podem ser exploradas. O primeiro passo é visualizar a impressão digital. Vários métodos de visualização são conhecidos na ciência forense. Um deles é a aplicação de um tipo de pó na impressão latente. O pó fixa à impressão e o restante que não fixa pode ser facilmente removido. Dessa forma, a impressão fica bem visível e pode até ser removida da superfície. A impressão latente é, então, digitalizada. A imagem é convertida para uma máscara preto e branco e impressa em

um filme transparente. É possível usar o filme como um molde, visto que o toner depositado forma elevações na sua superfície. Após o molde pronto, a impressão digital falsa é confeccionada usando cola, silicone, látex, etc (SOUSEDIK; BUSCH, 2014). A Figura 2.14 mostra os passos para criação de um *spoof* utilizando um método não-cooperativo.



Figura 2.14 – Processo de criação de um *spoof* de impressão digital pelo modo não cooperativo. Adaptado de (GHIANI et al., 2013).

2.6 Considerações Finais

Neste capítulo inicialmente foi introduzido o conceito de Biometria, foram apresentados exemplos das principais características biométricas humanas que podem ser utilizadas para o reconhecimento e os requisitos que estas características devem atender, na sequência foram explorados conceitos relacionados as impressões digitais, mostrando suas principais características e os tipos de sensores que podem ser utilizados para sua captura. Além disso, 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 descritos os ataques em sistemas biométricos baseados em impressões digitais com foco nos ataques do tipo *spoofing*.

No próximo capítulo encontram-se descritos os padrões responsáveis por auxiliar a detecção dos *spoofings* descritos neste capítulo.

Capítulo 3

TÉCNICA PROPOSTA

3.1 Considerações iniciais

Neste capítulo é descrita a técnica proposta para cumprir o objetivo principal, que é desenvolver um novo micropadrão espacial de imagens digitais a fim de que o mesmo aumente a precisão de métodos de detecção de fraudes em sistemas biométricos que fazem uso de impressões digitais. Define-se um micropadrão como sendo uma estrutura formada por pixels em seus respectivos níveis de cinza, com o qual se pode descrever um contexto espacial de alguma característica presente na imagem, como bordas, cantos, textura e até mesmo padrões mais complexos e abstratos. No método desenvolvido, os micropadrões são responsáveis pela representação de características mais abstratas, as quais são responsáveis por descrever propriedades que diferem impressões digitais falsificadas de impressões digitais verdadeiras. São descritas na seção 3.5 as configurações nas quais o método apresentado foi aplicado nas devidas bases de dados.

3.2 *Multi-Scale Local Binary Pattern (MSLBP)*

Nesta seção é descrito o primeiro micropadrão presente na literatura a ser definido em abordagens multiescalares. Sua utilização, inicialmente, era voltada ao reconhecimento e análise de texturas. Posteriormente, tal padrão foi empregado no uso de detecção de impressões digitais fraudulentas.

3.2.1 Abordagem Monoescalar

O método desenvolvido neste trabalho estende o conceito do padrão *Local Binary Pattern* (LBP), visto pela primeira vez na sua forma mais elementar em (OJALA; PIETIKÄINEN; HARWOOD, 1996). Tal padrão é extraído da vizinhança 3x3 de cada pixel presente na imagem. Posteriormente, o conceito foi estendido em (OJALA; PIETIKÄINEN; MÄENPÄÄ, 2002) de forma a permitir sua utilização em problemas que exigem tratamento com vizinhanças mais abrangentes, isto é, com dimensões superiores a 3x3. Deste modo, define-se o padrão através da equação (3.1):

$$LBP_{P,R} = \sum_{k=0}^{P-1} s(g_c - g_k) * 2^k, \quad (3.1)$$

em que P é o número de amostras (pixels $g_0, g_1, \dots, g_{P-1}$) igualmente espaçadas a uma distância R do pixel central g_c e presentes em sua vizinhança, e s é dada pela equação (3.2):

$$s(x) = \begin{cases} 1, & \text{se } x \geq 0, \\ 0, & \text{se } x < 0. \end{cases} \quad (3.2)$$

A Figura 3.1 exemplifica como é feito o cálculo do padrão LBP , que é a forma simplificada de denotar o valor $LBP_{8,1}$ dado na equação (3.1), em uma vizinhança 3x3 de um pixel.

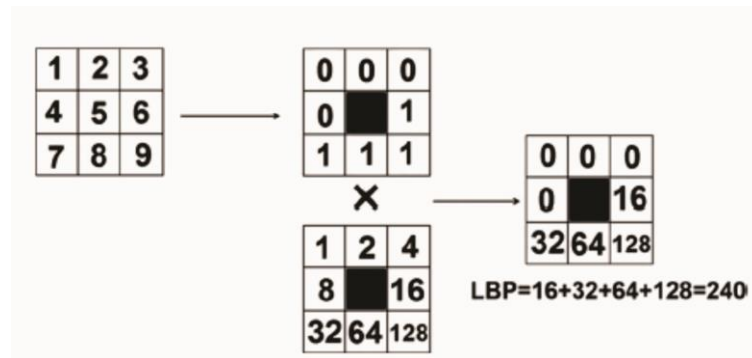


Figura 3.1 – Ilustração da extração do padrão LBP (JIA et al., 2014).

3.2.2 Abordagem Multiescalar

Em (MÄENPÄÄ; PIETIKÄINEN, 2003) é sugerido que se faça uso de extrações sucessivas do padrão $LBP_{P,R}$ (Figura 3.2) na mesma imagem. Cada extração é caracterizada

de acordo com o raio R . Métodos que fazem uso de estratégia semelhante são conhecidos como multiescalares (*multi-scale*) por apresentarem mais de uma etapa (escala) na extração da informação requerida.

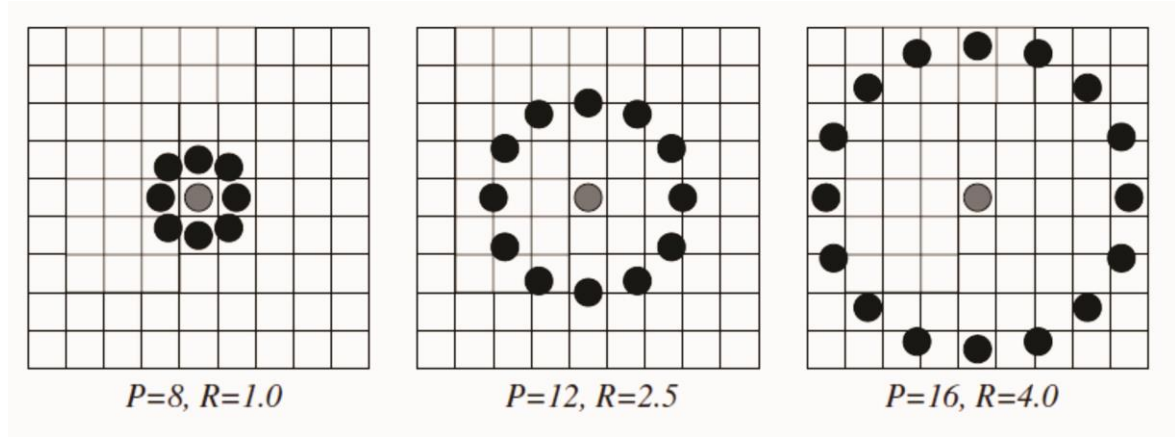


Figura 3.2 – Conjuntos de vizinhanças circulares simétricas (MÄENPÄÄ; PIETIKÄINEN, 2003).

JIA et al. (2014) apresentam duas variações de um método que faz uso de várias escalas e é conhecido como *Multi-Scale Local Binary Pattern* (MSLBP). A primeira versão, denominada no trabalho por MSLBP1, consiste de diversas extrações do padrão LBP_{8,R_n} de uma imagem suavizada por filtragem Gaussiana. Já a segunda versão, denominada no trabalho por MSLBP2, consiste de extrair o padrão $LBP_{8,1}$ de regiões as quais foram suavizadas por filtros de média, isto é, o cálculo do padrão $LBP_{8,1}$ não é feito utilizando-se pixels, mas fazendo uso de regiões que contém a média dos respectivos níveis de cinza dos pixels, como é exemplificado na Figura 3.3.

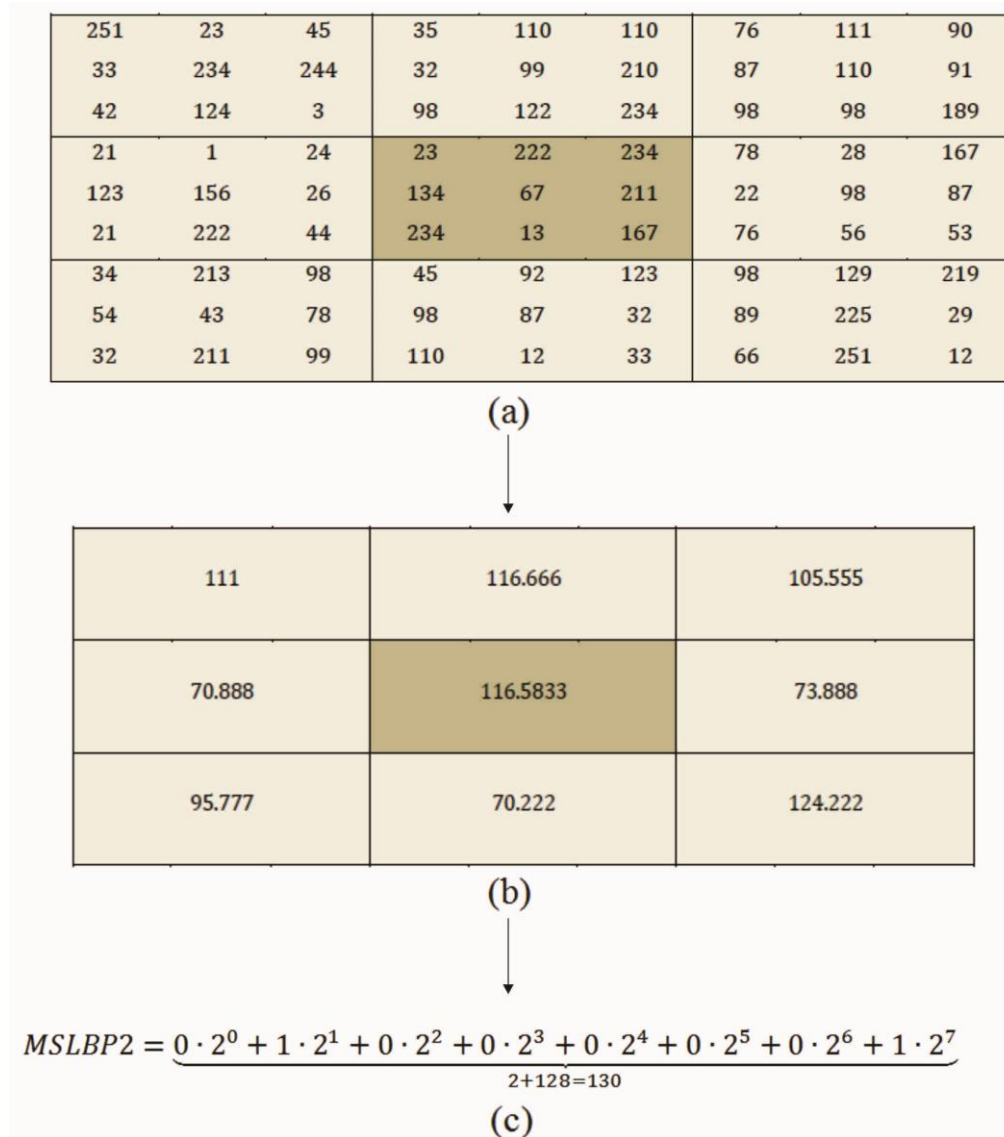


Figura 3.3 – Cálculo do MSLBP2 de uma matriz 9x9. (a) Matriz 9x9, (b) Média das regiões 3x3 da matriz original, (c) Cálculo do MSLBP2.

Este trabalho é baseado apenas na primeira variação do método MSLBP, o método MSLBP1, que consiste em extrair o padrão LBP_{8,R_n} da imagem suavizada por um filtro Gaussiano de tamanho G_n , dado pela equação (3.5), na n -ésima escala. Sendo que o desenvolvimento de cada escala se faz de acordo com a mudança dos valores dos raios. Tal mudança ocorre respeitando a distribuição ótima com relação à aplicação de filtros gaussianos apresentada em (MÄENPÄÄ; PIETIKÄINEN, 2003). A Figura 3.4 apresenta vizinhanças de um pixel central que são quantizadas por oito amostras ($P = 8$), formando oito setores que distam R_n do pixel central. A necessidade da filtragem Gaussiana presente no método se dá para que todos os pixels contidos nos círculos da Figura 3.4 sejam levados em consideração

no cálculo do micropadrão. Com a ação de um filtro passa-baixas, a informação de uma amostra é coletada em uma maior área, que no caso são os círculos da Figura 3.4. O raio externo da “área útil” das amostras formadas por círculos na Figura 3.4, que funciona como valor auxiliar no cálculo do raio R_n da operação LBP_{8,R_n} , é dado pela equação (3.3).

$$r_n = r_{n-1} \cdot \left(\frac{2}{1 - \sin \frac{\pi}{8}} - 1 \right), \quad n \in \{2, \dots, N\}, \quad (3.3)$$

na qual N é o número de escalas utilizadas no método, e P_n é o número de amostras utilizadas no cálculo de cada operação do padrão LBP_{P_n,R_n} , ou seja, $P_n = 8$ para qualquer n .

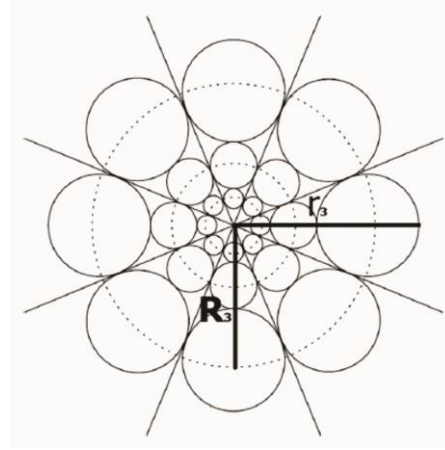


Figura 3.4 – Distribuição ótima dos raios do padrão MSLBP1 com respeito à redução de redundância da informação capturada pelo padrão. Fonte: (MÄENPÄÄ; PIETIKÄINEN, 2003).

Nota-se que é necessário que $r_n \geq 1$ para todo n , pois trata-se de um raio responsável por estabelecer distâncias entre um pixel central e a borda de suas vizinhanças. Desta forma, r_1 é definido por 1.5, que é a menor distância entre o centro e a borda de uma vizinhança 3x3.

Os raios das operações LBP_{8,R_n} são escolhidos de forma que as áreas efetivas (círculos da Figura 3.4) das amostras estejam em contato. Consequentemente, define-se R_n ($n \geq 2$) como sendo o ponto médio entre r_n e r_{n-1} :

$$R_n = \frac{r_n + r_{n-1}}{2}, \quad n \in \{2, \dots, N\}. \quad (3.4)$$

Como R_n representa a distância entre o pixel central e os pixels de suas vizinhanças, é natural que R_1 seja definido por 1, que é a menor distância entre o pixel central e os elementos de sua vizinhança 3x3.

Os valores r_n também são utilizados para calcular o tamanho das janelas utilizadas nos filtros Gaussianos, como mostra a equação (3.5):

$$G_n = 2 \cdot \left\lceil \frac{r_n - r_{n-1}}{2} \right\rceil + 1, \quad n \in \{2, \dots, N\}, \quad (3.5)$$

na qual a função $\lceil \cdot \rceil: \mathbb{R} \rightarrow \mathbb{N} \cup \{0\}$ é a função responsável por associar a um valor o menor inteiro que seja maior que o mesmo.

Em cada nível, o valor δ_n necessário para a aplicação do filtro Gaussiano é dado pela equação (3.6):

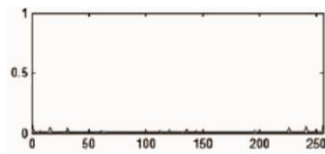
$$\delta_n = \frac{G_n}{\sqrt{-2\ln(0.05)}}, \quad n \in \{2, \dots, N\}. \quad (3.6)$$

3.2.3 Extração de características

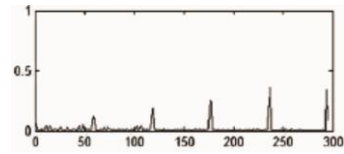
Inicialmente, o micropadrão LBP e suas formas estendidas, como o MSLBP, foram desenvolvidos a fim de analisar texturas em imagens. O trabalho de JIA et al. (2014) faz comparações entre histogramas gerados pelos micropadrões extraídos de impressões digitais legítimas e de impressões digitais forjadas. Obteve-se como conclusão que a diferença entre os histogramas gerados pelo padrão MSLBP1 é nítida, enquanto que os histogramas construídos a partir do padrão LBP são extremamente semelhantes, como pode ser observado na Figura 3.5. Isto é, a análise feita a partir de padrões com mais de uma escala é mais confiável. Assim, é natural que a extração de característica de métodos baseados em análise de textura seja feita a partir dos histogramas gerados pelos padrões utilizados.



Impressão Verdadeira



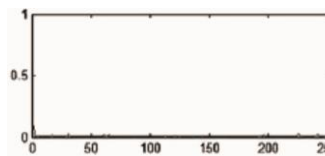
Histograma do LBP



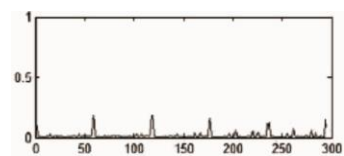
Histograma do MSLBP1



Impressão Falsificada



Histograma do LBP



Histograma do MSLBP1

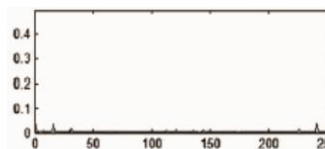
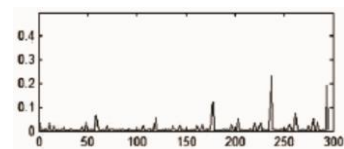
Diferença entre os
histogramas do padrão
LBPDiferença entre os
histogramas do padrão
MSLBP1

Figura 3.5 – Análise dos histogramas dos padrões LBP e MSLBP1 extraídos de uma impressão digital verdadeira e de uma impressão digital falsa. Adaptado de (JIA et al., 2014).

Pela equação (3.1), o padrão $LBP_{8,R}$ gera valores inteiros contidos na faixa $[0,255]$ para qualquer R calculado na equação (3.4). Em (OJALA; PIETIKÄINEN; MÄENPÄÄ, 2002) são apresentados e definidos alguns desses valores que representam uma classe especial chamada de *uniform patterns*. Tal classe é responsável, na grande maioria das vezes, pela caracterização de mais de 90% de toda informação que se pretende extrair. Define-se como *uniform pattern* o valor $U \in [0,255] \cap \mathbb{Z}$ tal que U escrito na sua forma binária $(b_1b_2b_3b_4b_5b_6b_7b_8)_2$, com $b_i \in \{0,1\}$, respeite a relação (3.7):

$$|b_1 - b_8| + \sum_{i=2}^8 |b_i - b_{i-1}| \leq 2. \quad (3.7)$$

JIA et al. (2014) afirma que, tomadas P amostras, existem $(P - 1) \cdot P + 2$ *uniform patterns*. Como $P = 8$ no método MSLBP1, então existem 58 valores entre $[0,255]$ que satisfazem a desigualdade (3.7).

Em cada escala do método MSLBP1 constrói-se o histograma dos valores gerados pelo padrão LBP_{8,R_n} extraído das imagens suavizadas pela filtragem Gaussiana. Posteriormente, tomam-se as taxas de ocorrência dos 58 *uniform patterns* no histograma construído na n -ésima escala seguidas da soma das taxas restantes para formar o vetor $x_n \in \mathbb{R}^{59}$. Finalmente, o vetor de características extraído de uma imagem pelo método MSLBP1 é o vetor $v = \text{norm}((x_1, \dots, x_N))$ cujo número de coordenadas é $N \cdot 59$, no qual N é o número de escalas utilizadas e $\text{norm}(\cdot)$ é a função responsável pela normalização apresentada na equação (3.8):

$$\text{norm}(y) = \frac{1}{\max(y) - \min(y)} (y - \min(y)). \quad (3.8)$$

Para cada imagem i de impressão digital, um vetor de características $v_i = \text{norm}((x_1^i, \dots, x_N^i))$ gerado pelo processo de extração de características citado no parágrafo anterior irá descrever as características biométricas da mesma. Desta forma, caso o padrão utilize N escalas e seja aplicado em M imagens de impressões digitais presentes em uma base de treinamento, então os vetores de características formam uma matriz, dada pela equação (3.9), que será utilizada para realizar o treinamento supervisionado de uma máquina de vetor de suporte (SVM).

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_M \end{bmatrix} = \begin{bmatrix} y_1^1 & y_2^1 & \cdots & y_N^1 \\ y_1^2 & y_2^2 & \cdots & y_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ y_1^M & y_2^M & \cdots & y_N^M \end{bmatrix}, \quad (3.9)$$

na qual, $y_j^i = \frac{1}{\max((x_1^i, \dots, x_N^i)) - \min((x_1^i, \dots, x_N^i))} (x_j^i - \min((x_1^i, \dots, x_N^i)))$.

SVM é um algoritmo de aprendizado de máquina muito eficiente, o qual é aplicado em muitas áreas de pesquisa. Tal algoritmo apresenta excelente performance em situações nas quais é necessária rotulação binária (XU, Q., 2014). Desta forma, seu uso no problema de detecção de fraudes em sistemas de impressões digitais se torna vantajoso, uma vez que as impressões digitais ou são autênticas ou são forjadas.

3.3 Local Mapped Pattern (LMP)

Inicialmente, o *Local Mapped Pattern* foi desenvolvido a fim de analisar texturas, recuperar imagens e auxiliar no reconhecimento de faces (FERRAZ; PEREIRA; GONZAGA, 2014). Neste trabalho, sua versão multiescala será utilizada para classificar impressões digitais.

A técnica LMP consiste na suavização dos níveis de cinza da imagem a partir do mapeamento feito através de uma função pré-definida. Desta forma, para cada pixel $g(i, j)$, calcula-se o mapeamento relativo $h(g(i, j))$ em função de uma região específica de vizinhos de $g(i, j)$. FERRAZ; JUNIOR; GONZAGA (2014) propõem que este mapeamento, definido em uma vizinhança $W \times W$ (Figura 3.6a), seja determinado pela equação (3.10):

$$h(g(i, j)) = \frac{\sum_{k=1}^W \sum_{l=1}^W (f_{g(i, j)}(g(k, l)) \cdot P(k, l))}{\sum_{k=1}^W \sum_{l=1}^W P(k, l)}, \quad (3.10)$$

na qual $f_{g(i, j)}$ é a função de mapeamento (Figura 3.6b) responsável pela suavização dos níveis de cinza da imagem (Figura 3.6a) que gerará os valores mapeados com relação ao pixel central dos $W^2 - 1$ vizinhos do pixel central $g(i, j)$ (Figura 3.6c) e P uma matriz de pesos $W \times W$ pré-definida (Figura 3.6d). Este mapeamento define o código LMP proposto que reflete a estrutura do micropadrão.

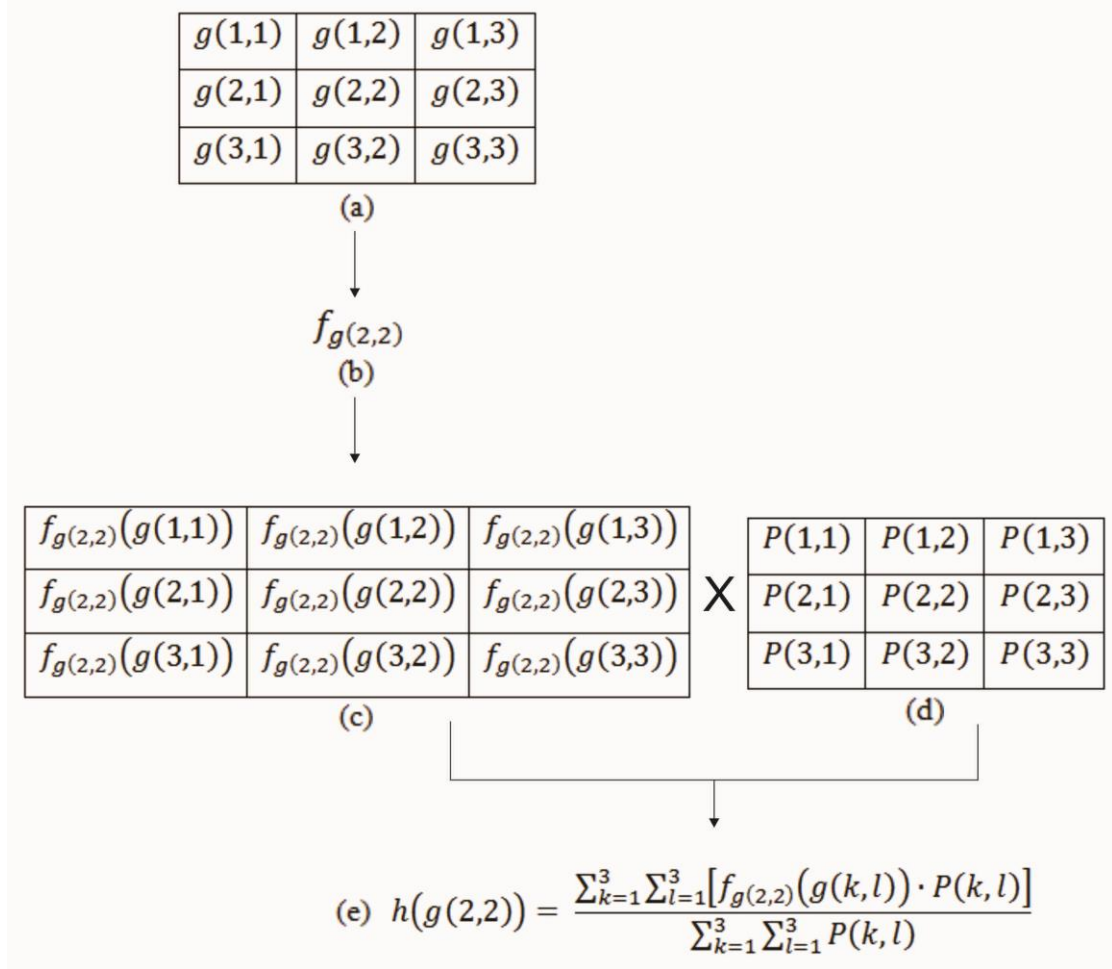


Figura 3.6 - Cálculo do mapeamento relativo do pixel central. (a) Vizinhança 3×3 do pixel central $g(2, 2)$, (b) Função de mapeamento, (c) Matriz dos mapeamentos realizados na vizinhança do pixel central, (d) Matriz de pesos, (e) Mapeamento relativo à vizinhança de $g(2, 2)$.

A equação (3.10) é uma generalização de outros métodos presentes na literatura. Como exemplo, o LBP descrito anteriormente pode ser obtido tomando a função $f_{g(i,j)}$ como a função degrau de Heaviside (H), dada pela equação (3.11):

$$H[A(k,l) - g(i,j)] = \begin{cases} 1, & \text{se } A(k,l) - g(i,j) \geq 0, \\ 0, & \text{se } A(k,l) - g(i,j) < 0. \end{cases} \quad (3.11)$$

Considerando o $LBP_{8,1}$ ($W = 3$), a matriz de pesos é dada por:

$$P = \begin{bmatrix} 1 & 2 & 4 \\ 8 & 0 & 16 \\ 32 & 64 & 128 \end{bmatrix}.$$

Para que os valores do padrão estejam em $[0,255]$ então é necessário fazer uso da normalização N_{LBP} , obtida pela equação (3.12):

$$N_{LBP} = \left[\underbrace{h(g(i,j))}_{\in[0,1]} \cdot \underbrace{\sum_{k=1}^W \sum_{l=1}^W P(k,l)}_{255} \right]. \quad (3.12)$$

3.4 Multi-Scale Local Mapped Pattern (MSLMP)

Como pode ser observado no trabalho de (JIA et al., 2014), as imagens de impressões digitais das bases LivDet2009 (MARCIALLIS et al., 2009), LivDet2011 (YAMBAY et al., 2012) e LivDet2013 (GHIANI et al., 2013) apresentam ruído em suas composições. Em (ZHU; WANG, 2012) vê-se que apenas a extração do padrão LBP de uma imagem o torna extremamente vulnerável a ruídos. No trabalho de JIA et al. (2014) este problema é amenizado com a utilização de filtros de característica passa-baixas antes de extrair versões de LBP apresentadas em (CHAN; KITTLER; MESSER, 2007). A partir desta ideia, a abordagem apresentada neste trabalho é uma extensão multiescala do método LMP apresentado em (FERRAZ; JUNIOR; GONZAGA, 2014). A proposta desta técnica é atenuar a ação ruidosa presente nas imagens de impressões digitais das bases citadas fazendo uso de aplicações responsáveis por suavizar as altas frequências presentes nas vizinhanças de um mesmo pixel. Tais vizinhanças seriam representadas por raios que aumentam conforme o nível do processo, caracterizando o método como um multiescala, que já se mostrou robusto na resolução de problemas envolvendo a detecção de impressões digitais fraudulentas em (JIA et al., 2014) e em (JIA et al., 2013).

Como visto na seção anterior, para utilizar o padrão LMP é necessário definir uma função $f_{g(i,j)}$ responsável pela suavização da imagem. Como na abordagem LBP é feita uma comparação *crisp* (0 ou 1) entre os pixels usando como aplicação de suavização a função degrau de Heaviside (Figura 3.7), há uma perda de informação, que é acentuada pela presença de ruído nas bases envolvidas, relacionada com a quantidade real da diferença entre os valores dos pixels. Assim, pretende-se, definindo $f_{g(i,j)}$ como função sigmoide (Figura 3.8), dada pela Equação (3.13), captar nuances que abordagens com formulação analítica não são capazes.

$$f_{g(i,j)}(A(k,l)) = \frac{1}{1 + e^{-\frac{A(k,l)-g(i,j)}{\lambda}}}, \quad \lambda \in (0,1]. \quad (3.13)$$

A aplicação de filtros gaussianos realizada no método MSLBP1 de JIA et al. (2014) torna-se desnecessária neste método, uma vez que a suavidade da função sigmoide transmite uma abordagem mais realística para o padrão LMP atenuando, assim, a perda de informação sofrida pela presença de ruído na imagem.

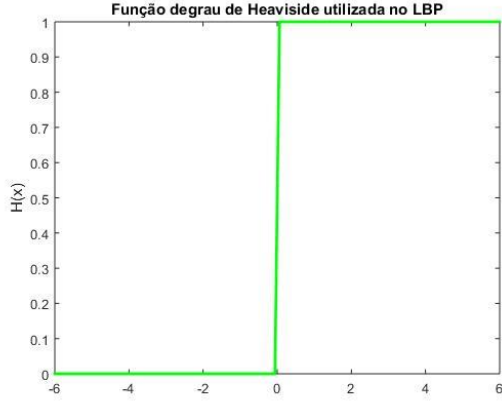


Figura 3.7 – Função degrau de Heaviside gerada pelo MATLAB.

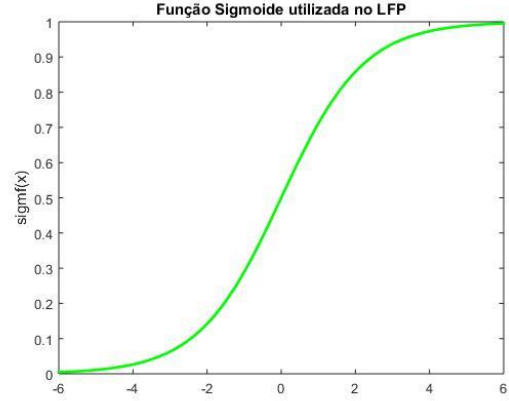


Figura 3.8 – Função sigmoide gerada pelo MATLAB.

No método aqui proposto, a evolução de cada escala se faz de acordo com o aumento do tamanho da dimensão das vizinhanças do pixel $g(i, j)$. Desta forma, a matriz de pesos P_n , descrita na Equação (3.15), será uma matriz $W_n \times W_n$ na n -ésima escala do método, com W_n dado pela Equação (3.14):

$$W_n = 2 \cdot [R_n] + 1, \quad (3.14)$$

na qual, R_n pode ser calculado através da equação (3.4).

$$P_n = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 0 & 0 & 0 & & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 0 & 0 & 0 & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & 0 & 0 & 0 & & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 0 & 0 & 0 & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 \end{bmatrix}. \quad (3.15)$$

A matriz P_n foi construída da maneira apresentada na equação (3.15) a fim de se assegurar que a abordagem proposta, assim como no método MSLBP1, fizesse uso de apenas 8 amostras pertencentes à vizinhança dos pixels em cada uma das escalas. Desta forma, a presença dos valores nulos em P_n é responsável por desconsiderar o valor de outros pixels

presentes na vizinhança do pixel central. Deste modo, os outros $W_n^2 - 8$ pixels são desconsiderados no cálculo do padrão MSLMP.

Logo, o padrão MSLMP de um pixel $g(i, j)$ na n -ésima escala do método é obtido através da equação (3.16):

$$\begin{aligned}
 MSLMP(g(i, j)) &= \frac{1}{8} \left(f_{g(i, j)}(A(1, 1)) + f_{g(i, j)}(A(1, [R_n] + 1)) + f_{g(i, j)}(A(1, W_n)) \right. \\
 &\quad + f_{g(i, j)}(A([R_n] + 1, 1)) + f_{g(i, j)}(A([R_n] + 1, W_n)) \\
 &\quad + f_{g(i, j)}(A(W_n, 1)) + f_{g(i, j)}(A(W_n, [R_n] + 1)) \\
 &\quad \left. + f_{g(i, j)}(A(W_n, W_n)) \right). \tag{3.16}
 \end{aligned}$$

Como a imagem da função sigmoide está compreendida entre 0 e 1, pela equação (3.16), tem-se $MSLMP(g(i, j)) \in (0, 1)$. Então, com o intuito de obter um padrão com valores inteiros em $[0, 255]$, o método faz uso da versão normalizada do valor obtido pela equação (3.16), isto é, o padrão final extraído do pixel $g(i, j)$ é o valor N_{MSLMP} calculado pela equação (3.17):

$$N_{MSLMP}(g(i, j)) = \lceil 255 \cdot MSLMP(g(i, j)) \rceil. \tag{3.17}$$

Após o cálculo do padrão N_{LMP} de todo pixel $g(i, j)$ de uma dada imagem, o vetor de características é construído e normalizado da mesma forma que o vetor x do método MSLBP1 de (JIA et al., 2014) descrito na seção 3.3. Finalmente, após toda imagem de impressão digital presente em uma base de dados de treinamento ter seu respectivo vetor de característica construído, forma-se uma matriz com estes vetores da mesma forma apresentada na equação (3.9). Para realizar o treinamento supervisionado faz-se uso de uma SVM linear.

3.4.1 Algoritmo da técnica proposta

Fazendo uso dos conceitos abordados nas seções anteriores, pode-se construir um algoritmo que represente a técnica de detecção de impressões digitais fraudulentas proposta. Este algoritmo está dividido em 8 etapas. Os Passos de 1 a 4 se referem ao cálculo do padrão MSLMP de uma imagem. No Passo 5 é feita a construção do vetor de características. No Passo 6 é feito o controle do fluxo do algoritmo de forma que possa ser construído um vetor de características para todas as imagens de uma dada base de dados. O Passo 7 é responsável

pela junção e normalização dos dados extraídos dos passos anteriores. Finalmente, no Passo 8 é feito o treinamento da SVM linear ou a classificação das imagens de teste.

A priori, define-se os parâmetros necessários para a utilização do método, no caso, qual sensor será avaliado, o valor λ da Equação (3.13), o valor inicial da matriz P_1 dada na Equação (3.15) e o número de escalas que se pretende fazer uso. Embora este último possa ser obtido de forma automática com métodos do tipo *k-fold cross validation*.

- Passo 1: Para cada pixel $g_m(i, j)$ da imagem g_m , calcula-se o padrão $N_{MSLMP}(g_m(i, j))$ descrito na Equação (3.17);
- Passo 2: Constrói-se um histograma intermediário formado pelos valores calculados no Passo 1;
- Passo 3: Tomam-se as taxas de ocorrência dos 58 *uniform patterns* (Equação 3.7) presentes no histograma construído no passo anterior, seguidas da soma das taxas restantes, para formar um vetor v_n^m de 59 coordenadas;
- Passo 4: Atualiza-se o valor de P_n conforme descrito na Equação (3.15) e repete-se os 3 primeiros Passos para $n = 2, \dots, N$, em que N é o número de escalas;
- Passo 5: Constrói-se o vetor $v^m = (v_1^m, v_2^m, \dots, v_N^m)$, que é o vetor de características da imagem g_m ;
- Passo 6: Repete-se os 5 primeiros Passos para $m = 2, \dots, M$, em que M representa o número de imagens da base de dados em questão;

- Passo 7: Constrói-se uma matriz de características $v = \begin{bmatrix} v^1 \\ v^2 \\ \vdots \\ v^M \end{bmatrix}$ e calcula-se sua

normalização $\bar{v}$ fazendo uso da função *norm* definida na Equação (3.8), isto é, $\bar{v} = \text{norm}(v)$;

- Passo 8: Caso a base de dados seja responsável pelo treinamento do classificador, então deve-se treiná-lo utilizando a matriz $\bar{v}$ obtida no Passo 7. Caso contrário, a matriz obtida no Passo 7 descreve as imagens pertencentes ao conjunto de testes. Sendo assim, o classificador após ter sido treinado deve determinar uma rotulação (impressão digital fraudulenta ou autêntica) para cada linha de $\bar{v}$, que corresponde a uma imagem na base de dados.

3.5 Metodologia aplicada

Os experimentos foram implementados no Matlab (MATHWORKS, 2014) R2013a na versão 64 bits, que fornece uma ampla biblioteca de funções, auxiliando em tarefas que demandariam maior tempo em outra linguagem de programação. O uso do Matlab agilizou o desenvolvimento da técnica proposta, auxiliando nas tarefas de processamento de imagens e no uso de técnicas de aprendizagem de máquina, imprescindíveis para o desenvolvimento deste trabalho. Foi utilizado também, um computador de 64 bits com processador de 2.4 GHZ e 4 GB de memória para execução dos experimentos.

Para que o padrão desenvolvido neste trabalho possa ser extraído de uma imagem, é necessário que se defina, a priori, um valor para o parâmetro λ apresentado na equação (3.13). Este valor define a qualidade do mapeamento feito na imagem quanto à questão da amenização do ruído presente nas bases de dados testadas. Empiricamente, o valor que se mostrou mais robusto sobre o mapeamento foi $\lambda = 0.25$. Em seguida, o padrão é extraído de todas as imagens de um mesmo sensor e, posteriormente, o classificador é treinado.

Cinco classificadores foram testados: *multilayer perceptron*, análise discriminante, árvore de decisão, k vizinhos mais próximos (KNN) e *Support Vector Machine* (SVM) de *kernel* linear, sendo que nenhum deles foi implementado neste trabalho visto que já se encontravam disponíveis no *software* Matlab. Como o classificador SVM apresentou os melhores resultados, este foi escolhido.

3.6 Considerações finais

Neste capítulo apresentou-se um novo padrão que faz uso de mais de uma escala e que tem como objetivo auxiliar a classificação de impressões digitais fraudulentas. O padrão proposto faz uso de técnicas presentes em outros padrões existentes na literatura as quais também foram descritas. A este novo padrão foi dado o nome de *Multi-Scale Local Mapped Pattern* (MSLMP) devido aos padrões dos quais seu desenvolvimento foi baseado. Também foram apresentadas na seção anterior as configurações utilizadas pela técnica proposta para a realização dos experimentos, cujos resultados serão apresentados no capítulo seguinte.

Capítulo 4

RESULTADOS E DISCUSSÕES

Neste capítulo são apresentados os experimentos realizados com a abordagem de extração de características realizada através do *Multi-Scale Local Mapped Pattern*. Na seção 4.1 são apresentadas também as métricas utilizadas para a avaliação do desempenho. Na Seção 4.2 as bases de dados usadas nos experimentos são descritas. Em seguida, na Seção 5.3, os resultados são apresentados e discutidos, e na mesma Seção o método proposto neste trabalho é comparado com algumas técnicas do estado da arte.

Tendo em vista a proximidade do assunto aqui abordado com o assunto abordado na dissertação de SILVA (2014) será utilizada a mesma disposição dos tópicos discutidos, assim como o texto contido em alguns parágrafos.

4.1 Medidas de desempenho

Algumas medidas foram utilizadas para medir o desempenho da técnica nas bases testadas e também para comparar os resultados com os obtidos em algumas técnicas do estado da arte que fazem uso das mesmas medidas, a saber: Taxa de falsa aceitação (*False Accept Rate* (FAR)), Taxa de falsa rejeição (*False Reject Rate* (FRR)), Média de Erro das Classificações (*Average Classification Error* (ACE)), que são bastante utilizadas por vários trabalhos presentes no estado da arte, por exemplo, (MARASCO; SANSONE, 2012); (PEREIRA et al., 2013); (TAN; SCHUCKERS, 2010); (JIA et al., 2013); (JIA et al., 2014); (GOTTSCHLICH et al., 2014). Tais medidas dizem respeito ao erro cometido pela técnica empregada, por esse motivo, quanto maior o valor delas pior será o desempenho da técnica avaliada. Todos os valores para o FAR, FRR e ACE apresentados neste trabalho são dados em porcentagem. Também é citada a taxa conhecida como Acurácia, que é responsável por

representar a taxa de acertos de uma técnica. Considera-se L_1 como o conjunto de imagens pertencentes à classe representante das impressões digitais, S_1 como sendo o conjunto de imagens de impressões digitais fraudulentas, L_2 o conjunto das imagens que foram classificadas como autênticas e S_2 as imagens que foram classificadas como fraudulentas em um determinado conjunto de imagens de teste (Δ). Considera-se ainda α como sendo a quantidade de imagens de dedos verdadeiros classificadas corretamente, ou seja, $\alpha = \#(L_1 \cap L_2)$; β representa a quantidade de imagens de dedos falsos classificadas como autênticos, isto é, $\beta = \#(S_1 \cap L_2)$; γ representa a quantidade de imagens de dedos verdadeiros classificados como fraudulentos, em outras palavras, $\gamma = \#(L_1 \cap S_2)$ e, finalmente, δ representa a quantidade de dedos falsos classificados corretamente, ou seja, $\delta = \#(S_1 \cap S_2)$. $\#(\cdot)$ é a função que representa a cardinalidade de um conjunto. A Tabela 4.1 mostra a descrição de como cada um desses valores são obtidos. A seguir as medidas utilizadas são apresentadas em detalhes.

Tabela 4.1 Quantidade de imagens por categoria

Classe/Classificação	L_2	S_2
L_1	α	γ
S_1	β	δ

4.1.1 False Accept Rate (FAR)

Taxa de falsa aceitação ou *False Accept Rate* (FAR) é a proporção de imagens de impressões digitais classificadas como verdadeiras, sendo que deveriam ter sido rejeitadas por serem imagens dedos falsos. Esta taxa é a responsável por quantizar os falsos positivos gerados pelo método. O valor FAR é obtido através da equação (4.1):

$$\text{FAR} = \frac{\beta}{\beta + \delta}. \quad (4.1)$$

4.1.2 False Reject Rate (FRR)

Taxa de falsa rejeição ou *False Reject Rate* (FRR) é a proporção de imagens de impressões digitais classificadas como fraudulentas, sendo que pertencem à classe de imagens legítimas. O valor FRR é obtido através da equação (4.2):

$$FRR = \frac{\gamma}{\gamma + \alpha} . \quad (4.2)$$

4.1.3 Average Classification Error (ACE)

Erro médio de classificação ou *Average Classification Error* (ACE) é dado pela média do FAR e FRR, calculados através das equações (4.1) e (4.2), respectivamente. O valor ACE é obtido através da equação (4.3):

$$ACE = \frac{FAR + FRR}{2} . \quad (4.3)$$

4.1.4 Acurácia (Acc)

A Acurácia é a medida responsável por estabelecer graus de precisão a um dado processo. Neste trabalho, esta taxa será definida pela equação (4.4):

$$Acc = \frac{\alpha + \delta}{\alpha + \beta + \gamma + \delta} . \quad (4.4)$$

A definição desta medida se torna necessária, pois a mesma é utilizada no trabalho de GOTTSCHLICH et al. (2014). Sendo assim, a comparação dos resultados obtidos pela técnica desenvolvida só se torna possível com a utilização da equação (4.4).

4.2 Bases de Dados

As bases de dados utilizadas nas avaliações realizadas no presente trabalho são resultados do esforço colaborativo entre dois centros de pesquisa: *Department of Electrical and Computer Engineering* da *Clarkson University* (EUA) e *Department of Electrical and Electronic Engineering* da *University of Cagliari* (Itália). Estas bases de dados foram confeccionada a fim de ser realizada uma competição mundial conhecida como *Liveness Detection Competition* que tem como objetivo avaliar algoritmos responsáveis por classificar e distinguir impressões digitais reais de impressões digitais forjadas. Cada uma dessas bases é

dividida em dois conjuntos: imagens de treinamento e imagens de teste, e os dois conjuntos são disjuntos para evitar resultados enviesados. As bases de dados são formadas por imagens de dedos verdadeiros e de dedos confeccionados com materiais sintéticos, tais como: gelatina, cola de madeira, silicone, entre outros. A saber:

- LivDet 2009, que é a base de dados que foi utilizada na primeira competição *Liveness Detection Competition* (MARCIALIS et al., 2009);
- LivDet 2011, que é a base de dados que foi utilizada na segunda edição da competição *Liveness Detection Competition* (YAMBAY et al., 2012);
- LivDet 2013, que é a base de dados que foi utilizada na terceira e última edição da competição *Liveness Detection Competition* cujos resultados foram publicados (GHIANI et al., 2013);
- LivDet 2015, que é a última base de dados lançada pela última edição da competição *Liveness Detection Competition*. No momento, só existe a base de treino disponível. Assim, a mesma foi dividida em duas partes iguais para que fosse feita a avaliação do método.

A seguir as bases de dados de cada competição são descritas.

4.2.1 LivDet2009

A LivDet 2009 é composta de três bases de dados: *Crossmatch*, *Identix* e *Biometrika*. A competição aconselha que em cada base de dados, 50% das imagens sejam destinadas ao treinamento e 50% para teste. A Tabela 4.2 apresenta as características das bases de dados dessa competição. Nessa tabela, as entradas *live* e *spoof* representam a quantidade de imagens de dedos verdadeiros e a quantidade de imagens de dedos falsos, respectivamente. Os dedos falsos usados nessa competição foram confeccionados com gelatina, silicone e massa de modelar. A Figura 4.1 apresenta exemplos de imagens dessa competição.

Tabela 4.2 - Características da base de dados LivDet 2009

Sensor	Modelo	Resolução (dpi)	Dimensões da Imagem	<i>live</i>	<i>spoof</i>
CrossMatch	Verifier 300LC	500	480 × 640	1500	1500
Identix	DFR2100	686	720 × 720	2000	2000
Biometrika	FX2000	569	312 × 372	2000	2000



(a) Impressão Digital verdadeira



(b) Dedo de silicone



(c) Dedo de gelatina



(d) Dedo de massinha de modelar

Figura 4.1 - Amostras de imagens usadas na LivDet 2009. Em (a) é apresentada a imagem de um dedo verdadeiro, obtida com um leitor biométrico. As demais imagens, (b), (c) e (d) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base.

4.2.2 LivDet2011

A LivDet 2011 é composta de quatro bases de dados: *Sagem*, *Digital Persona*, *Italdata* e *Biometrika*. Cada uma dessas bases possuem 4000 imagens e são divididas em dois conjuntos de mesmo tamanho, treinamento e teste. A Tabela 4.3 apresenta as características dessas bases de dados. Os dedos falsos usados nessa competição foram confeccionados com gelatina, látex, massa de modelar, silicone e cola de madeira para as bases *Digital Persona* e *Sagem*. Já nas bases *Biometrika* e *Italdata* os materiais usados foram: gelatina, látex, ecoflex, silicone e cola de madeira. A Figura 4.2 mostra exemplos de imagens dessa competição.

Tabela 4.3 - Características da base de dados LivDet 2011

Sensor	Modelo	Resolução (dpi)	Dimensões da Imagem	live	spoof
Sagem	MSO300	500	352 × 384	2000	2000
Digital Persona	400B	500	355 × 391	2000	2000
Biometrika	FX2000	500	312 × 372	2000	2000
Italdata	ET10	500	640 × 480	2000	2000



(a) Impressão
Digital
Verdadeira



(b) Impressão
Digital
verdadeira



(c) Impressão
Digital
Verdadeira



(d) Dedo de EcoFlex



(e) Dedo de
gelatina



(f) Dedo de Latex



(g) Dedo de
silicone



(h) Dedo de massinha de
modelar



(i) Dedo de cola de
madeira

Figura 4.2 - Amostras de imagens usadas na LivDet 2011. Em (a), (b) e (c) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base.

4.2.3 LivDet2013

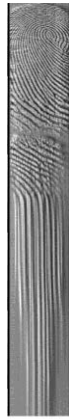
A LivDet 2013 foi a última versão da competição LivDet que teve seus resultados publicados. A competição é composta de quatro bases de dados: *Biometrika*, *Italdata*, *Crossmatch* e *Swipe*. Cada uma dessas bases possuem 4000 imagens e são divididas em dois conjuntos de mesmo tamanho, treinamento e teste. Na Tabela 4.4 são apresentadas as características dessas bases de dados. Os dedos falsos usados nessa competição foram confeccionados com *Body Double*, látex, massa de modelar e cola de madeira nas bases *Crossmatch* e *Swipe*. Já nas bases *Biometrika* e *Italdata*, os materiais usados foram: gelatina, látex, ecoflex, modasil e cola de madeira. Na Figura 4.3 pode-se observar exemplos de imagens dessa competição.

Tabela 4.4 - Características da base de dados LivDet 2013

Sensor	Modelo	Resolução (dpi)	Dimensões da Imagem	live	spoof
CrossMatch	L SCAN	500	800 × 750	2000	2000
	GUARDIAN				
Swipe	-	96	355 × 391	2000	2000
Biometrika	FX2000	569	312 × 372	2000	2000
Italdata	ET10	500	208 × 1500	2000	2000



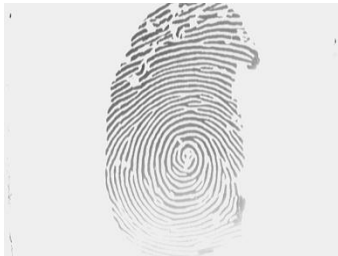
(a) Impressão
Digital
Verdadeira



(b) Impressão
Digital
verdadeira



(c) Dedo de modasil



(d) Dedo de EcoFlex



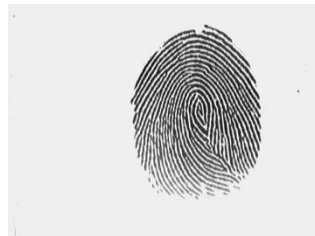
(e) Dedo de
gelatina



(f) Dedo de Latex



(g) Dedo de Body
Double



(h) Dedo de massinha de
modelar



(i) Dedo de cola de
madeira

Figura 4.3 - Amostras de imagens usadas na LivDet 2013. Em (a) e (b) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (c), (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base.

4.2.4 LivDet2015

A LivDet 2015 foi a última versão da competição LivDet. A competição é composta de quatro bases de dados: *Digital_Persona*, *GreenBit*, *Hi_Scan*, *Crossmatch* e *Time_Series*. As três primeiras bases possuem 2000 imagens. As características dos sensores utilizados na confecção dessas bases de dados não estão disponíveis para consulta. Os dedos falsos usados nessa competição foram confeccionados com *Body Double*, ecoflex e massa de modelar nas bases *Crossmatch* e *Time_Series*. Já nas bases *Digital_Persona*, *GreenBit* e *Hi_Scan*, os materiais usados foram: gelatina, látex, ecoflex, e cola de madeira. Na Figura 4.4 são apresentados exemplos de imagens dessa competição.



(a) Impressão Digital Verdadeira



(b) Impressão Digital verdadeira



(c) Impressão Digital verdadeira



(d) Dedo de EcoFlex



(e) Dedo de gelatina



(f) Dedo de Latex



(g) Dedo de Body Double



(h) Dedo de massinha de modelar



(i) Dedo de cola de madeira

Figura 4.4 - Amostras de imagens usadas na LivDet 2015. Em (a), (b) e (c) são apresentadas imagens de dedos verdadeiros, obtida com um leitor biométrico. As demais imagens, (d), (e), (f), (g), (h) e (i) são obtidas com dedos confeccionados com materiais sintéticos. As imagens não são necessariamente do mesmo dedo ou base.

4.3 Resultados

Nesta Seção serão apresentados os resultados da técnica proposta nas quatro bases da competição *Liveness Detection Competition* (LivDet) citadas na seção 4.3. O objetivo nesta seção é comparar a análise do MSLMP com as mais recentes técnicas que apresentam os melhores resultados até o momento, elas variam de base para base e por isso serão apresentada nas próximas seções. Experimentos foram realizados para cada base de dados e os resultados são mostrados nas próximas seções. Na Seção 4.4.1 são apresentados os resultados obtidos na base da LivDet 2009, na Seção 4.4.2 os resultados obtidos na LivDet 2011, enquanto que na Seção 4.4.3 tem-se os resultados obtidos na LivDet 2013 e a Seção 4.4.4 é dedicada aos resultados obtidos com a base LivDet 2015. Por fim, na Seção 4.4.5 é apresentada uma discussão sobre os resultados alcançados.

4.3.1 LivDet 2009

Nas bases dessa competição, o padrão MSLMP_ X , em que X é o número de escalas utilizadas, foi comparado com: o vencedor da LivDet 2009 (Anonymous2) (MARCIALIS et al., 2009), e as técnicas presentes nos trabalhos de MARASCO; SANSONE (2012), de GALBALLY et al. (2012), de OJALA; PIETIKÄINEN; MÄENPÄÄ (2000) (LBP), de OJANSIVU; RAHTU; HEIKKILA (2008) (LPQ), de (PEREIRA et al., 2013) (SSCA) e de GRAGNANIELLO et al. (2013) (WLD). Os resultados das demais técnicas foram obtidos do artigo de (GRAGNANIELLO et al., 2013), que faz uma comparação de algumas técnicas do estado da arte com o padrão *Weber Local Descriptor* (WLD) desenvolvido em seu trabalho. Na Tabela 4.5 são apresentados os resultados obtidos nas bases de dados dessa competição. Quanto menor o valor do ACE menor será o erro médio de classificação e mais precisa será a técnica que o apresentar.

Tabela 4.5 – Resultados obtidos nas bases da LivDet 2009

Técnica	Biometrika			Crossmatch			Identix		
	FAR	FRR	ACE	FAR	FRR	ACE	FAR	FRR	ACE
WLD	1,09	1,23	1,16	7,13	4,27	5,70	2,04	1,96	2,00
LPQ	5,32	4,91	5,12	5,33	6,60	5,97	2,00	3,47	2,73
Anonymous2	15,60	20,70	18,20	14,40	15,90	15,20	9,80	11,30	10,60
Marasco	12,20	13,00	12,60	17,40	12,90	15,20	8,30	11,00	9,70
LBP	52,18	4,57	28,38	7,20	9,73	8,47	5,02	5,38	5,20
SSCA	12,97	66,12	39,54	10,97	6,80	8,89	0,53	3,56	2,04
Galbally	3,10	71,80	37,40	8,80	20,80	14,80	4,80	5,00	4,90
MSLMP_1	8,00	8,40	8,20	16,00	17,46	16,73	2,85	1,95	2,40
MSLMP_2	5,60	6,53	6,07	11,7	16,45	14,08	2,35	1,60	1,95
MSLMP_3	3,06	3,87	3,47	10,65	10,85	10,75	2,45	1,45	1,95
MSLMP_4	2,93	4,00	3,47	10,65	10,80	10,73	2,30	1,35	1,83

Na base *Biometrika*, fazendo uso de apenas uma escala, o padrão MSLMP não supera apenas duas técnicas: WLD e LPQ. E, fazendo uso de apenas três escalas já supera a técnica LPQ.

Fazendo uso de 4 escalas, o método supera o vencedor da LivDet 2009, MARASCO; SANSONE (2012) e GALBALLY et al. (2012) na base *Crossmatch*.

E, com apenas duas escalas, o método supera todos os participantes na base *Identix*.

O desenvolvimento do método com respeito a suas escalas sugere que 3 escalas são suficientes para que a técnica proposta seja robusta nessa base de dados. Tendo em vista que o ganho na precisão de classificação não é significativo quando comparados os resultados referentes à penúltima e à última linha da Tabela 4.5, isto é, quando comparadas as performances de MSLMP_3 e de MSLMP_4.

4.3.2 LivDet 2011

Nessa base, o método proposto foi comparado com: o vencedor da LivDet 2011 (Dermalog), e as técnicas de MARASCO; SANSONE (2012), o LBP de MÄENPÄÄ; PIETIKÄINEN (2003), o LPQ de OJANSIVU; RAHTU; HEIKKILA (2008), o WLD de GRAGNANIELLO et al. (2013), o SSCA de PEREIRA et al. (2013), e finalmente, é feita uma comparação com as versões multiescala (MSLBP1 e MSLBP2) do padrão LBP do trabalho (JIA et al., 2014). Na Tabela 4.6 são apresentados os resultados obtidos na base LivDet 2011.

Tabela 4.6 – Resultados obtidos nas bases da LivDet 2011

Técnica	Biometrika			Italdata			Sagem			Digital Persona		
	FAR	FRR	ACE	FAR	FRR	ACE	FAR	FRR	ACE	FAR	FRR	ACE
LPQ	15,70	9,90	12,80	16,00	15,28	15,64	8,70	3,96	6,33	11,90	7,50	9,70
LBP	8,40	11,90	10,15	18,50	16,47	17,48	13,80	4,44	9,12	13,40	12,20	12,80
WLD	19,30	7,20	13,25	22,50	32,84	27,67	8,60	4,73	6,66	13,40	14,10	13,75
SSCA	15,90	25,80	20,80	18,20	33,50	25,80	11,30	14,40	12,80	22,10	8,70	15,40
Dermalog	11,00	29,00	20,00	15,10	28,50	21,80	15,10	12,50	13,80	66,00	6,20	36,10
Marasco	38,00	42,00	40,00	39,90	40,10	40,00	13,80	13,10	13,45	6,20	11,60	8,90
MSLBP1	-	-	7,30	-	-	14,80	-	-	5,3	-	-	2,5
MSLBP2	-	-	10,60	-	-	12,6	-	-	5,6	-	-	6,7
MSLMP_1	39,90	16,30	28,10	34,50	26,40	30,45	18,14	6,94	12,78	19,40	15,10	17,25
MSLMP_7	23,40	9,00	16,20	22,30	17,20	19,75	3,27	0,09	4,54	14,00	9,10	11,55
MSLMP_14	14,60	5,60	10,10	18,90	11,70	15,30	0,00	0,00	0,00	2,00	4,50	3,25

Percebe-se que o valor ACE de todas as bases de dados desta edição da *Liveness Detection Competition* é maior ao da edição comentada na subseção anterior. Desta forma, conclui-se que esta base representa um problema mais “difícil” de ser solucionado. Assim, foi necessário que o método fizesse uso de 14 escalas para que o mesmo apresentasse bons resultados.

Os resultados obtidos pela análise do método na base *Biometrika* evidenciaram que o método MSLMP é superior apenas ao método de MARASCO; SANSONE (2012) quando utilizada apenas uma escala em sua composição. Em contrapartida, quando o método é

formado por 14 escalas, a única técnica a apresentar resultados melhores é a que utiliza o padrão MSLBP1. Desta forma, os resultados sugerem que o método proposto tem um grande poder de adaptação.

Com respeito à base *Italdata*, nenhum método se mostra completamente satisfatório no estado da arte. Mesmo assim, apenas duas técnicas presentes na literatura se mostram superiores à técnica proposta: os métodos MSLBP1 e MSLBP2.

A base de dados *Sagem* apresenta resultados surpreendentes quando a técnica proposta faz uso de 14 camadas. Nenhuma imagem é classificada erroneamente. Sendo assim, o método se mostra superior a todos os outros na análise desta base.

O resultado da análise do padrão MSLMP com 14 escalas aplicado à base *Digital Persona* se mostra satisfatório, tendo em vista que apenas o método MSLBP1 apresenta um valor de ACE menor.

O MSLMP_14 apresenta o menor ACE médio em relação a todas as técnicas comparadas: 7,1625. Esse resultado mostra que, em média, o MSLMP supera todas as demais técnicas do estado da arte comparadas neste trabalho, inclusive a técnica WLD, que se mostrou superior à técnica proposta quando aplicada à base LivDet 2009 e mostrou um resultado pouco satisfatório quando aplicada à base em questão.

4.3.3 LivDet 2013

Nessas bases, o padrão proposto neste trabalho foi comparado com os três melhores algoritmos da 3ª edição da competição e com variações do método *Histograms of Invariant Gradients* (HIG) apresentados no trabalho de GOTTSCHLICH et al. (2014), que é o único trabalho no estado da arte que realiza experimentos em tal base de dados. Na Tabela 4.7 e na Tabela 4.8 são apresentados os resultados obtidos.

Tabela 4.7 – Comparação dos resultados obtidos nas bases da LivDet 2013

Técnica	Biometrika			Italdata			Crossmatch			Swipe		
	FAR	FRR	ACE	FAR	FRR	ACE	FAR	FRR	ACE	FAR	FRR	ACE
UniNap1	6,40	3,00	4,70	4,90	2,10	3,50	31,10	31,28	31,19	16,10	11,45	13,78
Dermalog	0,10	3,30	1,75	1,10	0,50	0,80	0,00	99,84	49,52	3,20	3,82	3,51
Anonimous2	1,30	1,80	1,55	1,00	0,20	0,60	0,30	98,40	49,35	9,60	2,50	6,05
MSLMP_1	1,00	4,00	2,50	1,00	4,00	2,50	67,44	9,6	38,52	10,66	20,40	15,53
MSLMP_2	0,50	3,50	2,00	0,50	3,50	2,00	99,76	0,20	49,98	4,33	15,00	9,67
MSLMP_7	0,10	0,10	0,10	0,10	0,10	0,10	99,60	0,24	49,95	3,12	7,50	5,31
MSLMP_14	0,00	0,00	0,00	0,00	0,00	0,00	99,28	0,20	49,74	2,77	4,10	3,44

Tabela 4.8 – Acurácia dos resultados obtidos nas bases da LivDet 2013

Técnica	Biometrika	Italdata	Crossmatch	Swipe
	Acc	Acc	Acc	Acc
HIG minutiae circle	95,70	89,40	60,04	67,59
HIG dense block packing	96,10	91,70	65,87	85,56
HIG dense block packing extended	89,10	98,30	71,24	81,59
HIG dense block packing combined	96,10	98,30	71,24	85,56
MSLMP_1	97,50	97,50	58,27	84,81
MSLMP_2	98,00	98,00	44,49	90,71
MSLMP_7	99,90	99,90	44,53	94,84
MSLMP_14	100,00	100,00	44,76	99,67

O método funciona exatamente igual nas bases *Biometrika* e *Italdata*. Nessas duas bases, uma única escala é suficiente para que o método funcione de maneira segura. Caso sejam utilizadas 7 escalas, o método é superior a todas as técnicas existentes na literatura. E caso sejam utilizadas 14 escalas, o classificador não erra nenhuma análise.

A base *Swipe* não é classificada tão facilmente pelo método MSLMP quando às bases *Biometrika* e *Italdata*, mas ainda é uma base da qual a técnica consegue se adaptar de maneira satisfatória já com 7 escalas. Além disso, com 14 escalas o método não é superado por nenhum resultado presente no estado da arte.

Já a base *Crossmatch*, que é a base com a maior média de erro ACE de todas as competições da LivDet, não funciona de forma satisfatória em nenhuma escala do método proposto neste trabalho, ainda que sua performance seja superior à de dois participantes da LivDet 2013. A base em questão ainda representa um problema muito difícil da área e permanece sem soluções seguras até a publicação deste trabalho.

4.3.4 LivDet 2015

Esta base ainda não oferece exemplares para testes. Até o momento, só estão disponíveis as imagens que seriam responsáveis pelo treinamento de classificadores. Desta forma, a base foi particionada em duas partes iguais para que fosse possível a realização de uma pré-avaliação a fim de obter uma perspectiva de como a técnica proposta reage às imagens dessa base. Como é apresentado na Tabela 4.9:

Tabela 4.9 – Comparação dos resultados obtidos nas bases da LivDet 2015

Técnica	Digital_Persona		Hi_Scan		GreenBit		Crossmatch		Time_Series	
	ACE	Acc	ACE	Acc	ACE	Acc	ACE	Acc	ACE	Acc
MSLMP_1	16,60	83,40	25,50	74,50	15,31	84,68	5,48	94,52	8,80	91,20
MSLMP_2	10,40	89,60	12,80	87,20	11,31	88,69	4,89	95,11	8,21	91,79
MSLMP_7	9,10	90,90	10,00	90,00	7,10	92,89	4,22	95,78	4,31	95,69

A base *Crossmatch* apresenta resultados muito bons quando a técnica faz uso de apenas uma escala, mas não apresenta melhora considerável conforme o número de escalas é aumentado.

O erro apresentado na classificação da base *Time-Series* foi reduzido, aproximadamente, pela metade quando o método faz uso de 7 escalas.

As bases *Digital_Persona*, *Hi_Scan* e *GreenBit* apresentam melhora considerável conforme o método faz uso de mais de uma escala, porém sugerem certa convergência em suas respectivas acurácias.

4.4 Considerações Finais

Neste capítulo as medidas de desempenho foram descritas a fim de que fosse possível realizar a comparação do método proposto com métodos presentes no estado da arte.

Também foram apresentadas as bases de dados utilizadas para avaliar a técnica proposta.

Nas bases da competição LivDet 2009 os resultados obtidos mostram que a técnica aqui proposta garante certa segurança em relação à maioria das técnicas comparadas. A técnica se mostrou robusta diante de bases de dados que não obtiveram bons resultados com apenas uma escala, que é o caso da *Biometrika* desta base.

A base LivDet é considerada uma base difícil de se trabalhar, tendo em vista que a média de seu ACE é elevada quando comparada às outras bases de impressões digitais LivDet. Ainda assim, o método se mostrou versátil e com grande capacidade de se adaptar a diferentes bases de dados, resultando no menor ACE médio comparado a outras técnicas.

O sensor cujas imagens representam um grande desafio na área de identificação de impressões digitais fraudulentas é o sensor responsável pela construção das imagens da base *Crossmatch* da LivDet 2013. Mesmo assim, o método proposto apresenta resultados superiores a duas técnicas vencedoras da referida edição da competição. Com relação às outras bases, a técnica aqui apresentada se mostrou segura e com resultados satisfatórios.

A base LivDet 2015 ainda não se apresenta em sua forma completa. Até o momento, apenas a base de treino foi disponibilizada pelos coordenadores da competição LivDet. Por isso, ainda que os resultados apresentados na Tabela 4.9 apresentem ACE médio inferior a 10%, o ideal seria realizar as análises na base de testes da LivDet 2015.

Capítulo 5

CONCLUSÕES

Uma técnica para detecção de impressões digitais falsas foi proposta, a versão multiescala do método *Local Mapped Pattern* (LMP), que foi chamada de Padrão Mapeado Localmente em Multiescala ou *Multi-Scale Local Mapped Pattern* (MSLMP). O MSLMP foi testado em quatro bases de dados: LivDet 2009, LivDet 2011, LivDet 2013 e LivDet 2015. A utilização dessas bases de dados torna mais fácil a comparação com outras técnicas do estado da arte, visto que várias abordagens propostas utilizam uma ou um conjunto delas nos seus experimentos (GOTTSCHLICH et al. 2014; MARASCO; SANSONE, 2012; GRAGNANIELLO et al., 2013; JIA et al. 2014). A técnica proposta neste trabalho obteve diferentes desempenhos nas bases de dados utilizadas. Nas bases da LivDet 2009, o MSLMP apresenta um dos melhores ACE médio, ficando com resultados piores que as técnicas LPQ e WLD, apenas. Esses resultados colocam o MSLMP como umas das técnicas mais eficientes para as bases de dados dessa competição. Nas bases da LivDet 2011, os resultados foram os mais satisfatórios, pois o MSLMP apresenta o menor ACE médio dentre todas as outras técnicas do estado da arte comparadas. Com isso a técnica proposta possui o melhor desempenho médio para essa competição. Já nas bases da LivDet 2013, o MSLMP não apresentou bons resultados na base *Crossmatch*, porém apresentou excelentes resultados nas outras bases. O método também se mostra promissor na base LivDet 2015, sendo que o mesmo apenas foi testado em uma partição meio a meio da base de treino, que é a única parte disponível até então da LivDet 2015.

5.1 Contribuições

A contribuição deste trabalho é apresentar uma abordagem para detecção de impressões digitais falsas, o MSLMP, que através de técnicas simples consegue resultados melhores ou comparáveis com técnicas apresentadas no estado da arte. Essa contribuição pode ser dividida nas seguintes partes:

- algoritmo simples, pois o método é baseado em uma variação do LBP de (MÄENPÄÄ; PIETIKÄINEN, 2003), amplamente utilizado em trabalhos de análise de textura e reconhecimento facial;
- aplicação da técnica nas quatro bases de dados disponíveis da LivDet e dessa forma contribuir para que outras técnicas propostas possam comparar seus desempenhos com o MSLMP em todas essas bases de dados;
- contribuir com o estado da arte melhorando os resultados obtidos até o presente momento. O MSLMP consegue superar alguns dos melhores resultados do estado da arte, o que representa uma contribuição importante para o avanço das pesquisas na área de detecção de impressões digitais falsas.

5.2 Trabalhos Futuros

Como pode-se notar na Seção 4.4, os resultados apresentados pelo MSLMP diferem razoavelmente dependendo da base de dados que é utilizada. As razões pelas quais os resultados diferem não foram bem compreendidas neste trabalho, como exemplo, tem-se que o método funciona muito bem fazendo uso de 14 escalas com respeito à análise das bases *Biometrika* e *Italdata* presentes na LivDet 2013, porém apresenta baixo desempenho para a base *Crossmatch*. Provavelmente isso ocorre devido às diferenças de textura das imagens dessas bases de dados ou à engenharia do sensor em si (Figura 5.1), que tem como característica a captura de impressões digitais com inclinação variável, isto é, as impressões digitais são digitalizadas sem orientação pré-definida, o que não é prejudicial no processo de casamento de minúcias descrito no Capítulo 2, mas pode ser prejudicial na distinção de impressões digitais verdadeiras e fraudulentas. Processos responsáveis por padronizar a orientação da impressão digital capturada podem ser empregados no método a fim de avaliar

se tal problema é atenuado, no entanto mais estudos precisam ser realizados a fim de compreender e explicar tal fenômeno para que se possa propor melhorias.



Figura 5.1 – Scanner L Guardian R2 da crossmatch.

O método proposto estabelece empiricamente que $\lambda = 0.25$ na equação (3.13). Isto é, após uma sequência de testes, conclui-se que um valor ao qual λ torna o método robusto é 0.25, porém técnicas mais precisas de otimização podem ser empregadas a fim de estabelecer um melhor valor para este parâmetro. Como exemplo, técnicas de Algoritmo Genético podem ser utilizadas a fim de se obter um valor que torne o método aqui apresentado mais funcional, versátil e, conseqüentemente, mais adaptativo.

Trabalhos como o de BHANARKAR et al. (2013) mostram que impressões digitais fraudulentas tendem a apresentar uma superfície mais áspera e rugosa, o que diminui a frequência das cristas da impressão digital. Desta forma, medidas responsáveis por descrever os padrões formados pela variação de cristas e vales em uma impressão digital, como a *X-Signature* (HONG; YIFEI; JAIN, 1998), podem ser acopladas à técnica proposta para obter melhores resultados.

Este método foi enviado para avaliação na competição LivDet 2015 e pretende-se que seja enviado novamente, após algumas melhorias, para uma possível competição LivDet 2017 a fim de avaliar as técnicas aqui discutidas.

REFERÊNCIAS

AL-AJLAN, A. Survey on fingerprint liveness detection. **2013 International Workshop on Biometrics and Forensics, IWBF 2013**, 2013.

ASHBOURN, J. **Biometrics: Advanced Identity Verification - The Complete Guide**. 1st ed. London: Springer, 2002.

BHANARKAR, A.; DOSHI, P.; ABHYANKAR, A.; BANG, A. Joint Time Frequency Analysis Based Liveness Fingerprint Detection. , p. 166–169, 2013.

BIGGIO, B.; AKHTAR, Z.; FUMERA, G.; MARCIALIS, G. L.; ROLI, F. Security evaluation of biometric authentication systems under real spoofing attacks. **IET Biometrics**, v. 1, n. 1, p. 11, 2012.

CASTRO, T. S. Identificação de Impressões Digitais Baseada na Extração de Minúcias. Dissertação de Mestrado. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

CHAN, C.; KITTLER, J.; MESSER, K. Multi-scale local binary pattern histograms for face recognition. **Proceedings of ICB**, p. 809–818, 2007. Disponível em: <<http://www.springerlink.com/index/558H766730557237.pdf>>. .

DAUGMAN, J. Recognizing Persons by Their Iris Patterns. , 1996. Springer US.

ELECCION, M. Pattern Recognition - Automatic Fingerprint Identification. **IEEE Spectrum**, p. 33–45, 1973.

FBI: FEDERAL BUREAU OF INVESTIGATION. The Science of Fingerprint: Classification and Uses. **U.S. Government Printing Oce**, 1984. Washington.

FERRAZ, C. T.; JUNIOR, O. P.; GONZAGA, A. Feature description based on Mean Local Mapped Pattern. **Workshop de Visão Computacional - WVC 2014**, v. X, p. 32–37, 2014.

FERRAZ, C. T.; PEREIRA, O.; GONZAGA, A. Feature description based on center-symmetric local mapped patterns. **Proceedings of the 29th Annual ACM Symposium on Applied Computing - SAC '14**, p. 39–44, 2014. Disponível em: <<http://dl.acm.org/citation.cfm?doid=2554850.2554895>>. .

GALBALLY, J.; ALONSO-FERNANDEZ, F.; FIERREZ, J.; ORTEGA-GARCIA, J. A high performance fingerprint liveness detection method based on quality related features. **Future Generation Computer Systems**, v. 28, n. 1, p. 311–321, 2012. Elsevier B.V. Disponível em: <<http://dx.doi.org/10.1016/j.future.2010.11.024>>. .

GALBALLY, J.; MARCEL, S.; FIERREZ, J. Image quality assessment for fake biometric detection: Application to Iris, fingerprint, and face recognition. **IEEE Transactions on Image Processing**, v. 23, n. 2, p. 710–724, 2014.

GALBALLY-HERRERO, J.; FIERREZ-AGUILAR, J.; RODRIGUEZ-GONZALEZ, J. D.; ALONSO-FERNANDEZ, F.; et al. On the vulnerability of fingerprint verification systems to fake fingerprints attacks. **Proceedings - International Carnahan Conference on Security Technology**, p. 130–136, 2006.

GALTON, F. **Finger Prints**. London: McMillan, 1892.

GHIANI, L.; YAMBAY, D.; MURA, V.; TOCCO, S.; et al. LivDet 2013 Fingerprint Liveness Detection Competition 2013. **Biometrics (ICB), 2013 International Conference on Biometrics Compendium**, p. 1–6, 2013.

GOTTSCHLICH, C.; MARASCO, E.; YANG, A. Y.; CUKIC, B. Fingerprint liveness detection based on histograms of invariant gradients. IEEE International Joint Conference on Biometrics. **Anais...** . p.1–7, 2014. Disponível em: <<http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6996224>>. .

GRAGNANIELLO, D.; POGGI, G.; SANSONE, C.; VERDOLIVA, L. Fingerprint liveness detection based on Weber Local image Descriptor. **2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, BioMS 2013 - Proceedings**, 2013.

GRAGNANIELLO, D.; VERDOLIVA, L.; POGGI, G.; SANSONE, C. Wavelet-Markov local descriptor for detecting fake fingerprints. **Electronics Letters**, v. 50, n. 6, p. 439–441, 2014. Disponível em: <<http://digital-library.theiet.org/content/journals/10.1049/el.2013.4044>>. .

HENRY, E. R. Classification and Uses of Fingerprints. **Wyman and Sons Ltda**, 1905.

HONG, L.; YIFEI, W.; JAIN, A. Fingerprint image enhancement: algorithm and performance evaluation. **Pattern Analysis and Machine Intelligence, IEEE Transactions on**, v. 20, n. 8, p. 777–789, 1998. Disponível em: <<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=709565>>. .

JAIN, A.; FLYNN, P.; ROSS, A. **Handbook of biometrics**. Springer, 2007.

JAIN, A.; HONG, L.; BOLLE, R. On-line fingerprint verification. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 19, n. 4, p. 302–314, 1997.

JIA, X.; YANG, X.; CAO, K.; ZANG, Y.; et al. Multi-scale local binary pattern with filters for spoof fingerprint detection. **Information Sciences**, v. 268, p. 91–102, 2014. Elsevier Inc. Disponível em: <<http://linkinghub.elsevier.com/retrieve/pii/S0020025513004787>>. .

JIA, X.; YANG, X.; ZANG, Y.; ZHANG, N.; et al. Multi-scale block local ternary patterns for fingerprints vitality detection. **Proceedings - 2013 International Conference on Biometrics, ICB 2013**, 2013.

KEHDY, C. **Exercícios de Dactiloscopia**. 2nd ed. São Paulo, 1968.

KRISHAN, K.; KANCHAN, T.; BUMBRAH, G. S. The Fingerprint Sourcebook. **Journal of Forensic and Legal Medicine**, v. 19, n. 3, p. 182–183, 2012.

MÄENPÄÄ, T.; PIETIKÄINEN, M. Multi-scale binary patterns for texture analysis. **Scia** **2003**, p. 885–892, 2003. Disponível em: <<http://dl.acm.org/citation.cfm?id=1763974.1764109>>. .

MALTONI, D.; MAIO, D.; JAIN, A. K.; PRABHAKAR, S. **Handbook of Fingerprint Recognition**. 2nd ed. Springer, 2009.

MARASCO, E.; SANSONE, C. Combining perspiration- and morphology-based static features for fingerprint liveness detection. **Pattern Recognition Letters**, v. 33, n. 9, p. 1148–1156, 2012. Elsevier B.V. Disponível em: <<http://dx.doi.org/10.1016/j.patrec.2012.01.009>>. .

MARCIALIS, G. L.; LEWICKE, A.; TAN, B.; COLI, P.; et al. First International Fingerprint Liveness Detection Competition—LivDet 2009. , 2009.

MATSUMOTO, H.; MATSUMOTO, Y.; KOJI, S.; HOSHINO, T. Impact of artificial “gummy” fingers on fingerprint systems. **Datenschutz und Datensicherheit**, p. 26(8), 2002.

MOON, Y. S.; CHEN, J. S.; CHAN, K. C.; SO, K.; WOO, K. C. Wavelet based fingerprint liveness detection. **ELECTRONICS LETTERS**, v. 41, n. 20, p. 2–3, 2006. Disponível em: <<http://discovery.ucl.ac.uk/45673/>>. .

OJALA, T.; PIETIKÄINEN, M.; HARWOOD, D. A comparative study of texture measures with classification based on featured distributions. **Pattern Recognition**, v. 29, n. 1, p. 51–59, 1996.

OJALA, T.; PIETIKÄINEN, M.; MÄENPÄÄ, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 24, n. 7, p. 971–987, 2002.

OJANSIVU, V.; RAHTU, E.; HEIKKILA, J. Rotation invariant local phase quantization for blur insensitive texture analysis. **2008 19th International Conference on Pattern Recognition**, p. 1–4, 2008.

PAES, C. Perícia identifica digitais em dedos de silicone usados por médicos. Disponível em: <<http://g1.globo.com/sp/mogi-das-cruzes-suzano/noticia/2013/03/pericia-identifica-digitais-em-dedos-de-silicone-usados-por-medicos.html>>. .

PANKANTI, S.; MEMBER, S.; PRABHAKAR, S. On the Individuality of Fingerprints : Models and Methods. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 24, n. i, p. 1010–1025, 2002.

PEIXOTO, G.; LOURENÇO, F. Médica do Samu é detida com seis dedos de silicone, em Ferraz. Disponível em: <<http://g1.globo.com/sp/mogi-das-cruzes-suzano/noticia/2013/03/medica-do-samu-e-detida-com-seis-dedos-de-silicone-em-ferraz.html>>. .

PEREIRA, L. F. A.; CAVALCANTI, G. D. C.; REN, T. I.; PINHEIRO, H. N. B. Spatial surface coarseness analysis: technique for fingerprint spoof detection. **Electronics Letters**, v. 49, n. 4, p. 260–261, 2013. Disponível em: <<http://digital-library.theiet.org/content/journals/10.1049/el.2012.4173>>. .

SCHNEIER, B. The uses and abuses of meta-analysis. **Family practice**, v. 13, n. 4, p. 397–401, 1999.

SILVA, J. J. O. Spatial Entropy Analysis (SEnA): uma técnica para detecção de impressões digitais falsas. Dissertação de Mestrado. Universidade Federal de Pernambuco, Recife, 2014.

SOUSEDIK, C.; BUSCH, C. Presentation attack detection methods for fingerprint recognition systems: A survey. **IET Biometrics**, , n. October, p. 1–15, 2014. Disponível em: <<http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2013.0020>>. .

TAN, B.; SCHUCKERS, S. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. **Pattern Recognition**, v. 43, n. 8, p. 2845–2857, 2010. Elsevier. Disponível em: <<http://dx.doi.org/10.1016/j.patcog.2010.01.023>>. .

USMANI, Z.-H.; IRUM, S.; AFZAL, H.; MAHMUD, S. How to Build an Automated Fingerprint Identification System. **2013 International Symposium on Biometrics and Security Technologies**, p. 40–47, 2013. Disponível em: <<http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6597664>>. .

XIAO, Q.; RAAFAT, H. Fingerprint Image Postprocessing: A combined statistical and structural approach. **Pattern Recognition**, v. 24, n. 10, p. 985–992, 1991.

XU, Q. Multiclass feature selection algorithms base on R-SVM. **Signal and Information Processing**, v. 1, n. 1, p. 525 - 529, 2014.

YAMBAY, D.; GHIANI, L.; DENTI, P.; MARCIALIS, G. L.; et al. LivDet 2011 - Fingerprint liveness detection competition 2011. **Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012**, p. 208–215, 2012.

ZHU, C.; WANG, R. Local multiple patterns based multiresolution gray-scale and rotation invariant texture classification. **Information Sciences**, v. 187, n. 1, p. 93–108, 2012. Elsevier Inc. Disponível em: <<http://dx.doi.org/10.1016/j.ins.2011.10.014>>. .

PROGRAMAÇÃO NO MATLAB

A.1 Rotina para o cálculo do LMP

```
function LMP_Im = LMP(Input_Im, lambda, R)

    if size(Input_Im, 3) == 3
        Input_Im = rgb2gray(Input_Im);
    end;

    R = ceil(R); %% R representa o raio da escala.
    L = 2*R + 1; %% L = W: tamanho da vizinhança.

    C = round(L/2);
    Input_Im = uint8(Input_Im);
    row_max = size(Input_Im,1)-L+1;
    col_max = size(Input_Im,2)-L+1;
    LMP_Im = zeros(row_max, col_max);

    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    P = ones(L,L); %% Define-se a matriz de pesos
    P(C,C) = 0;

    S = 8; %% sum(sum(P));
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    for i = 1:row_max
        for j = 1:col_max

            A = Input_Im(i:i+L-1, j:j+L-1);
            A = double(A);
            c = A(C,C);

            %% Calcula-se o padrão LMP(c) multiplicado por 255
            %% u(x,c,lambda) = sigmf(x,[lambda c]); é a função sigmoide.
            LMP_Im(i,j) = 255*(u(A(1,1), c, lambda)*P(1,1) + u(A(1,C), c,
lambda)*P(1,C) + u(A(1,L), c, lambda)*P(1,L) + u(A(C,1), c, lambda)*P(C,1)
+ u(A(C,L), c, lambda)*P(C,L) + u(A(L,1), c, lambda)*P(L,1) + u(A(L,C), c,
lambda)*P(L,C) + u(A(L,L), c, lambda)*P(L,L))/S;

        end;
    end;
```

```

end;

%% Finalmente, tem-se o padrão  $N_{\{LMP\}}(g)$ 
LMP_Im = round(LMP_Im);

end

```

A.2 Rotina para a construção da matriz de características de uma base de dados

```

function [feat] = extracao_de_padrao(grp, max_escala, lambda)
%% max_escala representa o número de escalas escolhido.

%% Em cada escala são armazenados 59 valores.
tam_escala = 59;

%% grp é a base de dados da qual será extraída o padrão MSLMP.
[N, ~] = size(grp);

%% Agora define-se os labels dos possíveis valores de MSLMP das
imagens.
% (0,0,0,0,0,0,0,0) ~> 0
% (1,0,0,0,0,0,0,0) ~> 1
% (1,1,0,0,0,0,0,0) ~> 3
% ...
% (1,1,1,1,1,1,1,1) ~> 255
labels = 0:255;

%% Matriz de características.
feat = zeros(N,max_escala*tam_escala);

%% Vetor dos uniform patterns.
U1 =
[0,1,2,3,4,6,7,8,12,14,15,16,24,28,30,31,32,48,56,60,62,63,64,96,112,120,12
4,126,127,128,129,131,135,143,159,191,192,193,195,199,207,223,224,225,227,2
31,239,240,241,243,247,248,249,251,252,253,254,255];

%% Definição dos raios utilizados nas escalas.
Rn = [1 2 3 5 7 11 13 17 19 23 29 61 89 137];

%%%%%%%%% Extração das características de cada imagem. %%%%%%%%%%
for i = 1:N
    %Leitura da i-ésima imagem.
    im = imread(grp{i});

    i_escala = 1;
    for escala = 1:max_escala
        disp(strcat('Scale: ',num2str(escala)));
        L = LMP(im, lambda, Rn(escala));

        %% Calcula-se o histograma da matriz dos MSLMPs.
        hist = histograma(labels, L);
    end
end

```

```

    %% Toma-se como característica o histograma dos padrões
    %% uniformes e depois se soma os não uniformes.
    for i_max = 1:58
        feat(i,i_escala) = hist(U1(i_max)+1);
        %% Este valor será zerado para não influenciar na soma
        %% depois.
        hist(U1(i_max)+1) = 0;
        i_escala = i_escala+1;
    end

    %% Soma dos valores restantes do histograma.
    feat(i,i_escala) = sum(hist);

    %% Passe para a próxima escala.
    i_escala = i_escala+1;
end
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
end

```

A.3 Rotina responsável por normalizar a matriz de características

```

function [feat] = normaliza(feat)

[N,~] = size(feat);

%Normalização dos dados.
for k = 1:N
    xkn = feat(k,:);
    minF = min(xkn);
    maxF = max(xkn);
    if (maxF-minF) ~= 0
        xkn = (xkn-minF)/(maxF-minF);
    end
    feat(k,:) = xkn;
end

end

```

A.4 Rotina responsável por definir de qual base de dados será extraído o padrão MSLMP

```
function roteiro_extracao_de_padrao( train, test, ano, base, metodo, lambda,
max_escala_LFP )
%% Define-se as imagens de treino e de teste de uma base.
[grp_Train, grp_Test, ~, ~, ~, ~] = readImPathTaT(ano, base);

if train == 1
    feat_Train = extracao_de_padrao(grp_Train, max_escala_LFP, lambda);

    feat_Train = normaliza(feat_Train);

    %% Grava-se em um arquivo txt a matriz de características extraída.
    gravaMatriz(feat_Train,
    strcat('C:\TrainPatterns2\',ano,'_',metodo,'_TRAIN_MULTSCALE_',base,'_lambda',num2str(lambda),'.txt'));

end

if test == 1
    feat_Test = extracao_de_padrao4(grp_Test, max_escala_LFP, lambda);

    feat_Test = normaliza(feat_Test);

    %% Grava-se em um arquivo txt a matriz de características extraída.
    gravaMatriz(feat_Test, strcat('C:\TestPatterns2\',ano,'_',metodo,'_TEST_MULTSCALE_',base,'_lambda',num2str(lambda),'.txt'));

end
end
```

A.5 Rotina responsável por treinar e classificar bases de dados

```
function [ Acc,FAR,FRR, ACE ] = train_classify( featTrain, featTest,
bTrain, bTest )

%% Treina-se a SVM Linear, com convergência de, no máximo, 1500000
iterações.
options.MaxIter = 1500000;
SVMStruct = svmtrain(featTrain,bTrain,'options',options);

%% Faz-se a classificação da base de testes.
r = svmclassify(SVMStruct,featTest);

%% Obtém-se um relatório da classificação obtida.
show = 0;
[ Acc,FAR,FRR, ACE ] = getreport( bTest, r, show );

End
```

A.6 Rotina que gera relatório da classificação obtida

```
function [ ac,fp,fn,ACE ] = getreport( b, r, show )

ac=0;fp=0;fn=0;
for i=1:size(r,1)
    if r(i)==1 && b(i)==-1
        fp = fp + 1;
    elseif r(i)==-1 && b(i)==1
        fn = fn + 1;
    else
        ac = ac + 1;
    end
end

n = size(b,1);
neg = 0; pos = 0;
for i=1:n
    if b(i) > 0
        pos = pos + 1;
    else
        neg = neg + 1;
    end
end
ACE = (fp/neg+fn/pos)/2;

if show == 1
    disp('Falsos negativos:~> ');
    disp(fn);
    disp('Falsos positivos:~> ');
    disp(fp);
    disp('Acertos:~> ');
    disp(ac);
    disp('Acurácia:~> ');
    disp(ac/n);
    disp('ACE:~> ');
    disp(ACE);
end

end
```