



Ministério da Justiça



UnB



**Centro de Apoio ao
Desenvolvimento
Tecnológico**



latitude
Laboratório de tecnologias da tomada de decisão

Termo de Cooperação/Projeto:

**Acordo de Cooperação Técnica
FUB/CDT e MJ/SE
Registro de Identidade Civil –
Replanejamento e Novo Projeto Piloto**

Documento:

**RT das 6 (seis) Biometrias Prováveis
de Utilização no RIC**

Data de Emissão:

10/06/2014

Elaborado por:

**Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento
Tecnológico – CDT
Laboratório de Tecnologias da Tomada
de Decisão – LATITUDE.UnB**

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Márcia Pelegrini
Secretária Executiva

Hélio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

EQUIPE TÉCNICA

Ana Maria da Consolação Gomes Lindgren
Alexandre Cardoso de Barros
Andréa Benoliel de Lima
Beatriz Merguiso Garrido
Celso Pereira Salgado
Delluiz Simões de Brito
Domingos Soares dos Santos
Elaine Fabiano Tocantins
Felipe Bragança Itaborahy
Fernando Saliba
Fernando Teodoro Filho
Guilherme Braz Carneiro
Jhon Kennedy Férrer Lima
José Alberto Sousa Torres
Joaquim de Oliveira Machado
Marcelo Martins Villar
Narumi Pereira Lima
Paulo Cesar Vieira dos Santos
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento
Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da
Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA

Flávio Elias Gomes de Deus
(Pesquisador Sênior)
William Ferreira Giozza
(Pesquisador Sênior)
Ademir Agostinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Andréia Campos Santana
Andreia Guedes Oliveira
Caio Rondon Botelo de Carvalho
Cristiane Faiad de Moura
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Eduarda Simões Veloso Freire
Egmar Alves da Rocha
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
João Luiz Xavier M. de Negreiros
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
José Elenilson Cruz
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Maria do Socorro Rocha
Pedro Augusto Oliveira de Paula
Renata Elisa Medeiros Jordão
Roberto Mariano de Oliveira Soares
Sandro Augusto Pavlik Haddad
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Valério Aymoré Martins
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
26/05/2014	0.1	Versão inicial
07/06/2014	0.2	Versão com todas as biometrias revisadas, faltando apenas a reescrita dos plágios detectados.
09/06/2014	0.3	Revisão inicial do texto, com reescrita dos plágios.
10/06/2014	0.4	Relatório final.



Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1	INTRODUÇÃO	11
1.1	Justificativa.....	12
1.2	Objetivos	12
1.3	Premissas.....	12
1.4	Metodologia.....	14
2	NOÇÕES SOBRE DESEMPENHO DE SISTEMAS BIOMÉTRICOS	18
2.1	Introdução.....	18
2.2	Valores de Desempenho – Taxas de Erro	19
2.3	Detalhamento das medidas estatísticas – Métricas de Desempenho	21
2.4	Principais tipos de erros	29
2.5	De-duplicação.....	31
3	ASSINATURA.....	32
3.1	INTRODUÇÃO.....	32
3.2	CARACTERÍSTICAS TÉCNICAS	35
3.2.1	Universalidade.....	35
3.2.2	Singularidade.....	36
3.2.3	Permanência	36
3.2.4	Coletabilidade.....	36
3.2.5	Desempenho	37
3.2.6	Aceitabilidade.....	37
3.2.7	Resistência à fraude	37
3.3	ESTIMATIVA DE CUSTO	38
3.4	CARACTERÍSTICAS DA COLETA	39
3.4.1	Idade inicial	39
3.4.2	Tamanho do arquivo gerado	39
3.4.3	Tempo de coleta.....	39
3.5	ALGORITMOS DE RECONHECIMENTO	39
3.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	40
3.7	UTILIZAÇÃO EM OUTROS PAÍSES	40
3.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	40
3.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	40
4	FACE	42
4.1	INTRODUÇÃO.....	42

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.4/125
--------------------	---------------------	---	------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

4.1.1	Etapas do processo de reconhecimento.....	43
4.2	CARACTERÍSTICAS TÉCNICAS	44
4.2.1	Universalidade	44
4.2.2	Singularidade.....	44
4.2.3	Permanência	44
4.2.4	Coletabilidade.....	45
4.2.5	Desempenho	45
4.2.6	Aceitabilidade.....	46
4.2.7	Resistência à fraude	46
4.3	ESTIMATIVA DE CUSTO	46
4.4	CARACTERÍSTICAS DA COLETA	47
4.4.1	Idade inicial	47
4.4.2	Tamanho do arquivo gerado	47
4.4.3	Tempo de coleta.....	48
4.5	ALGORITMOS DE RECONHECIMENTO	48
4.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	48
4.7	UTILIZAÇÃO EM OUTROS PAÍSES	48
4.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	48
4.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	49
5	IMPRESSÃO DIGITAL.....	50
5.1	INTRODUÇÃO.....	50
5.2	CARACTERÍSTICAS TÉCNICAS	58
5.2.1	Universalidade	58
5.2.2	Singularidade.....	59
5.2.3	Permanência	59
5.2.4	Coletabilidade.....	59
5.2.5	Desempenho	60
5.2.6	Aceitabilidade.....	62
5.2.7	Resistência à fraude	62
5.3	ESTIMATIVA DE CUSTO	63
5.4	CARACTERÍSTICAS DA COLETA	64
5.4.1	Idade inicial	64
5.4.2	Tamanho do arquivo gerado	64
5.4.3	Tempo de coleta.....	64
5.5	ALGORITMOS DE RECONHECIMENTO	65
5.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	65

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.5/125
--------------------	---------------------	---	-----------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

5.7	UTILIZAÇÃO EM OUTROS PAÍSES	66
5.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	66
5.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	67
6	ÍRIS	68
6.1	INTRODUÇÃO	68
6.2	CARACTERÍSTICAS TÉCNICAS	72
6.2.1	Universalidade	72
6.2.2	Singularidade	72
6.2.3	Permanência	73
6.2.4	Coletabilidade	73
6.2.5	Desempenho	74
6.2.6	Aceitabilidade	76
6.2.7	Resistência à fraude	77
6.3	ESTIMATIVA DE CUSTO	78
6.4	CARACTERÍSTICAS DA COLETA	79
6.4.1	Idade inicial	79
6.4.2	Tamanho do arquivo gerado	79
6.4.3	Tempo de coleta	79
6.5	ALGORITMOS DE RECONHECIMENTO	80
6.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	80
6.7	UTILIZAÇÃO EM OUTROS PAÍSES	80
6.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	81
6.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	81
7	VEIAS DA MÃO	82
7.1	INTRODUÇÃO	82
7.2	CARACTERÍSTICAS TÉCNICAS	87
7.2.1	Universalidade	87
7.2.2	Singularidade	87
7.2.3	Permanência	88
7.2.4	Coletabilidade	89
7.2.5	Desempenho	89
7.2.6	Aceitabilidade	90
7.2.7	Resistência à fraude	91
7.3	ESTIMATIVA DE CUSTO	91
7.4	CARACTERÍSTICAS DA COLETA	91
7.4.1	Idade inicial	91

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.6/125
--------------------	---------------------	---	------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

7.4.2	Tamanho do arquivo gerado	92
7.4.3	Tempo de coleta	92
7.5	ALGORITMOS DE RECONHECIMENTO	92
7.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	93
7.7	UTILIZAÇÃO EM OUTROS PAÍSES	93
7.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	94
7.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	94
8	VOZ	95
8.1	INTRODUÇÃO	95
8.2	CARACTERÍSTICAS TÉCNICAS	98
8.2.1	Universalidade	98
8.2.2	Singularidade	99
8.2.3	Permanência	99
8.2.4	Coletabilidade	99
8.2.5	Desempenho	100
8.2.6	Aceitabilidade	101
8.2.7	Resistência à fraude	102
8.3	ESTIMATIVA DE CUSTO	102
8.4	CARACTERÍSTICAS DA COLETA	102
8.4.1	Idade inicial	102
8.4.2	Tamanho do arquivo gerado	102
8.4.3	Tempo de coleta	102
8.5	ALGORITMOS DE RECONHECIMENTO	103
8.6	CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA	104
8.7	UTILIZAÇÃO EM OUTROS PAÍSES	104
8.8	UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO	104
8.9	RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC	104
9	CONCLUSÃO	106
	ANEXO I – MAPAS MENTAIS	109
	REFERÊNCIAS BIBLIOGRÁFICAS	116

ABREVIACÕES

ABIS	<i>Automated Biometric Identification System</i>
AFIS	<i>Automated Fingerprint Identification System</i>
CER	<i>Crossover Equal Rate</i>
DET	<i>Detection Error Trade-off</i>
EER	<i>Equal Error Rate</i>
FAR	<i>False Acceptance Rate</i>
FRR	<i>False Rejection Rate</i>
FTA	<i>Failure to Acquire</i>
FTC	<i>Failure to Capture</i>
FTD	<i>Failure to Detect</i>
FTE	<i>Failure to Enroll</i>
FTP	<i>Failure to Process</i>
FNMR	<i>False Non-Match Rate</i>
FMR	<i>False Match Rate</i>
GAR	<i>Genuine Acceptance Rate</i>
ICE	<i>Iris Challenge Evaluation</i>
ROC	<i>Receiver Operating Characteristic</i>
SDK	<i>Software Development Kit</i>
TTM	<i>Time to Match</i>
TTE	<i>Time to Enroll</i>

FIGURAS

Figura 1 – Fluxograma da Metodologia de Trabalho do Grupo de Biometria	16
Figura 2 – Curvas DET das principais tecnologias biométricas.....	27
Figura 3 – Fluxograma do processo de reconhecimento facial	44
Figura 4 – Histórico do reconhecimento da impressão digital	50
Figura 5 – Tipos de pontos característicos ou minúcias.....	52
Figura 6 – Sistemas de linhas das impressões digitais.....	53
Figura 7 – Regiões da impressão digital e pontos singulares, marcados em vermelho.....	54
Figura 8 – Deltas e linhas utilizados na classificação e verificação das impressões digitais.....	54
Figura 9 – Exemplo e etapas de transformação da imagem direcional.....	55
Figura 10 – Valores FAR (FNMR) e FMR (FRR) para impressão digital	61
Figura 11 – Resultado do pré-processamento da imagem da íris.	70
Figura 12 – Taxas de FAR e FRR para a biometria da íris.....	74
Figura 13 – Probabilidades individuais de Falsa Aceitação e Falsa Rejeição.....	76
Figura 14 – Aquisição de imagem das veias da mão por meio de câmera térmica em ambiente com temperatura de 20° a 25° C	83
Figura 15 – Aquisição de imagem das veias da mão por meio de câmera térmica em ambiente com temperatura de 30° a 35° C	84
Figura 16 – Imagem das veias da mão antes e depois da normalização	85
Figura 17 – Imagem das veias da mão antes e depois da segmentação	85
Figura 18 – Imagem das veias da mão antes e depois da Skeletonization	86
Figura 19 – Tipos de sistemas de reconhecimento da fala (voz).	97
Figura 20 – Taxas FAR e FRR para a biometria voz.	101
Figura 21 – Percentual de brasileiros potenciais não portadores de impressão digital e íris.	107

TABELAS

Tabela 1 – Definições utilizadas no documento	18
Tabela 2 – Fatores que afetam a performance dos sistemas biométricos.....	21
Tabela 3 – Exemplos de desempenho de sistemas biométricos.....	28
Tabela 4 – Exemplos de desempenho de sistemas biométricos.....	30
Tabela 5 – FRVT2002: Avaliação comercial do sistema de reconhecimento facial 2D.	45
Tabela 6 – FRVT2006: Avaliação comercial dos sistemas de reconhecimento facial 2D e 3D.	46
Tabela 7 – Estimativa do custo da face.	47
Tabela 8 – Estimativa do custo da impressão digital.	63
Tabela 9 – Custo da íris do projeto indiano.....	78
Tabela 10 – Estimativa do custo da íris.....	79

1 INTRODUÇÃO

O relatório ora apresentado foi elaborado a partir de revisão bibliográfica no intuito de aprofundar aspectos técnicos referentes às seis biometrias consideradas mais promissoras segundo (Jain e Pankanti, 2008) e principalmente ao relatório “Panorama Geral das Biometrias” (Buiati, 2014), quais sejam: assinatura, face, impressão digital, íris, veias da mão e voz. Essa escolha também está embasada em outras situações particulares: o fato do estado de São Paulo utilizar um sistema de voz em alguns serviços de autenticação; a assinatura ser usada como atesto em documentos em geral; a utilização das veias da mão por instituição financeira como um mecanismo de identificação desde o começo de 2007.

Este documento está organizado da seguinte forma: inicialmente é feita a apresentação do estado atual do Subprojeto de Controle Biométrico balizando seu escopo, objetivo, premissa e metodologia adotada; subsequentemente são apresentados conceitos básicos e noções sobre desempenho em sistemas biométricos; a seguir é realizado o detalhamento de cada uma das seis biometrias anteriormente citadas, adotando uma sistemática comum de descrição que engloba características técnicas, segurança, situação em outros países e custo, dentre outras; e por último, são apresentadas recomendações e justificativas da aplicabilidade dessas biometrias no Programa RIC.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.11/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

1.1 Justificativa

De acordo com a estrutura do Programa RIC, a equipe técnica responsável pelas diretrizes relacionadas à escolha das biometrias a serem utilizadas, juntamente com a equipe da Universidade de Brasília, têm como requisito o desenvolvimento desse trabalho para dar subsídio e auxílio à tomada de decisão pelo Comitê Gestor.

1.2 Objetivos

O objetivo deste documento é apresentar dados técnicos relevantes para subsidiar a tomada de decisão sobre as biometrias a serem aplicadas pelo sistema de identificação biométrico brasileiro.

1.3 Premissas

O estudo bibliográfico realizado baseou-se na produção científica de autores renomados na área de biometria. Dentre eles, destacam-se:

- **Anil K. Jain:** professor da Universidade do Estado de Michigan¹, conhecido por suas contribuições nos campos de reconhecimentos de padrão, visão computacional e reconhecimento biométrico. Portador de seis patentes norte americanas em comparação de impressão digital e duas patentes coreanas sobre vigilância. Também é autor de vários livros, tais como: “*Introduction to Biometrics*” (2011), “*Handbook of Biometrics*” (2007), “*Handbook of Multibiometrics*” (2006), “*Handbook of Face Recognition*” (2011), “*Handbook of Fingerprint Recognition*” (2009), “*Markov Random Fields: Theory and Applications*” (1993), e “*Algorithms For Clustering Data*” (1988). Também participou como consultor na especificação do sistema biométrico indiano (UIDAI). Atualmente, o autor possui mais de 100.000 citações no Google acadêmico².
- **John Daugman:** professor de Visão Computacional e Reconhecimento de Padrão na Universidade de Cambridge, Faculdade de Ciência de Computação

¹ Anil K. Jain, Universidade de Michigan, <http://www.cse.msu.edu/~jain/>

² Google Acadêmico, Anil K. Jain, http://scholar.google.com.br/citations?user=g-_ZXGsAAAAJ&hl=pt-BR&oi=ao

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.12/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

e Tecnologia³. Conhecido pelo trabalho pioneiro em neurociência computacional e pela invenção do algoritmo de reconhecimento de íris baseado em *wavelet 2D de Gabor*. É co-fundador e membro de conselho da *Iridian Technologies*, companhia líder em pesquisa, desenvolvimento e venda de tecnologias de autenticação baseadas no reconhecimento de íris.

- **Arun Ross:** professor associado no Departamento de Ciência da Computação e Engenharia na Universidade do Estado de Michigan. Sua pesquisa inclui reconhecimento de padrão, fusão classificatória, aprendizado de máquina, visão computacional e biometria. Co-autor do livro "*Introduction to Biometrics*" e "*Handbook of Multibiometrics*", e co-editou o livro "*Handbook of Biometrics*".
- **Karthik Nandakumar:** trabalhou sob a tutela de Anil K. Jain no Grupo de Pesquisa de Biometria no Laboratório de Reconhecimento de Padrão e Processamento de Imagem (PRIP) na Universidade do Estado de Michigan. Também é co-autor dos livros "*Introduction to Biometrics*" e "*Handbook of Multibiometrics*", junto de Anil K. Jain e A. Ross.

Como balizadores de dados de desempenho dos sistemas biométricos estudados, foram utilizadas, principalmente, as informações fornecidas pelas competições do NIST (*National Institute of Standards and Technology*), realizadas em intervalos de tempo pré-determinados. Essas competições promovem a inovação e a competitividade industrial entre os fabricantes de equipamentos biométricos e são utilizadas como referências em diversos países. FpVTE (*Fingerprint Vendor Technology*)⁴, IREX (*Iris Exchange*)⁵ e FRVT (*Face Recognition Vendor Technology*)⁶ são as principais competições realizadas pelo NIST, as quais referem-se à impressão digital, íris e face, respectivamente.

Outra premissa considerada refere-se ao estudo de caso de implementações bem sucedidas por outros países como Índia, México, Indonésia, entre outros, devido ao tamanho de suas populações em comparação à população brasileira. Ademais, existem similaridades desses programas com a realidade brasileira como: legado da impressão digital no sistema eleitoral mexicano, população rural da Índia, etc. Portanto, no

³ John Daugman, Universidade de Cambridge, <http://www.cl.cam.ac.uk/~jgd1000/>

⁴ <http://www.nist.gov/itl/iad/ig/fpvt2012.cfm>

⁵ <http://www.nist.gov/itl/iad/ig/irex.cfm>

⁶ <http://www.nist.gov/itl/iad/ig/frvt-2013.cfm>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.13/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

desenvolvimento deste estudo, foram enfatizados projetos de identificação biométricos de grande escala.

Em virtude da dificuldade de realizar um estudo técnico detalhado incluindo simulações e provas de conceito com amostras representativas, este trabalho apresenta uma exaustiva e objetiva revisão bibliográfica sistematizada para a criação de parâmetros de aplicação em projetos de grande escala, sendo os pilares que conduziram tais estudos:

- incremento da amostra populacional cadastrada, no caso de algum indivíduo não possuir uma determinada biometria, visando oferecer acesso a todas as camadas sociais aos serviços essenciais;
- provimento de uma maior segurança contra fraudes e ataques maliciosos, exigindo que o impostor tenha que violar duas ou mais biometrias;
- aumento da precisão global do sistema considerando o processo de deduplicação da base de dados como meio de garantir a unicidade dos cadastros do sistema.

1.4 Metodologia

A metodologia adotada no presente trabalho ao mesmo tempo que criou os pilares e premissas supracitados, também os utilizou como suporte ao longo de seu desenvolvimento. Desta forma, durante sua construção, foram desenvolvidas as seguintes etapas, as quais estabeleceram três grandes marcos.

1º. Marco: o primeiro marco foi estabelecido com o Relatório “Panorama Geral sobre Biometrias” (Buiati, 2014). Para a elaboração do referido relatório foram executadas as seguintes atividades.

- Seleção de estudos de caso de identificação civil no mundo com foco em sistemas de grande escala;
- Visita a países com algumas características similares ao Brasil, como México e Índia;
- Definição dos requisitos necessários para a condução da pesquisa bibliográfica, ou seja, parâmetros de interesse a serem explorados no relatório;
- Levantamento das referências bibliográficas e demais fontes de informações de interesse;

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.14/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

- E finalmente a elaboração do texto do referido relatório.

2º. Marco: para o desenvolvimento do segundo marco foi inicialmente efetuada a eleição das seis principais biometrias elencadas no Relatório “Panorama Geral sobre Biometrias”, ou seja, assinatura, face, impressão digital, íris, veias da mão e voz. Em seguida, foi efetuado um questionário com as diretrizes a serem desenvolvidas, estudadas e detalhadas, as quais permitiram subsidiar a tomada de decisão sobre as biometrias aplicáveis ao sistema de identificação civil brasileiro. Para o desenvolvimento do presente relatório, referente ao 2º. Marco, foi, então, estabelecido um grupo de estudo constituído de quatro servidores do Ministério da Justiça e três pesquisadores da Universidade de Brasília. Este grupo manteve-se reunido diariamente por 8 semanas consecutivas, desde o dia 22 de abril até 13 de junho de 2014, pesquisando, estudando e discutindo as seis biometrias elencadas. Concomitantemente, foram efetuadas apresentações quinzenais das biometrias estudadas, mapas mentais, contatos e discussões com especialistas conceituados na área, tanto de universidades brasileiras (Campinas – 21 a 23/05 e Curitiba – 06/06), como de universidades internacionais (Michigan – 10/06), além de instituições como o Departamento de Polícia Federal (20/05) e Banco Itaú (11/06). Subsequentemente, a partir dos relatórios individuais de cada uma das seis biometrias foi elaborado este relatório.

No presente momento consolida-se o 2º. Marco com a apresentação do Relatório sobre Biometrias.

3º. Marco: Para a execução do 3º. Marco far-se-á a apresentação deste documento para o Comitê Gestor, objetivando sua aprovação, deliberação e consequente definição das biometrias a serem utilizadas no Programa RIC, conforme apresentado na Figura 1.

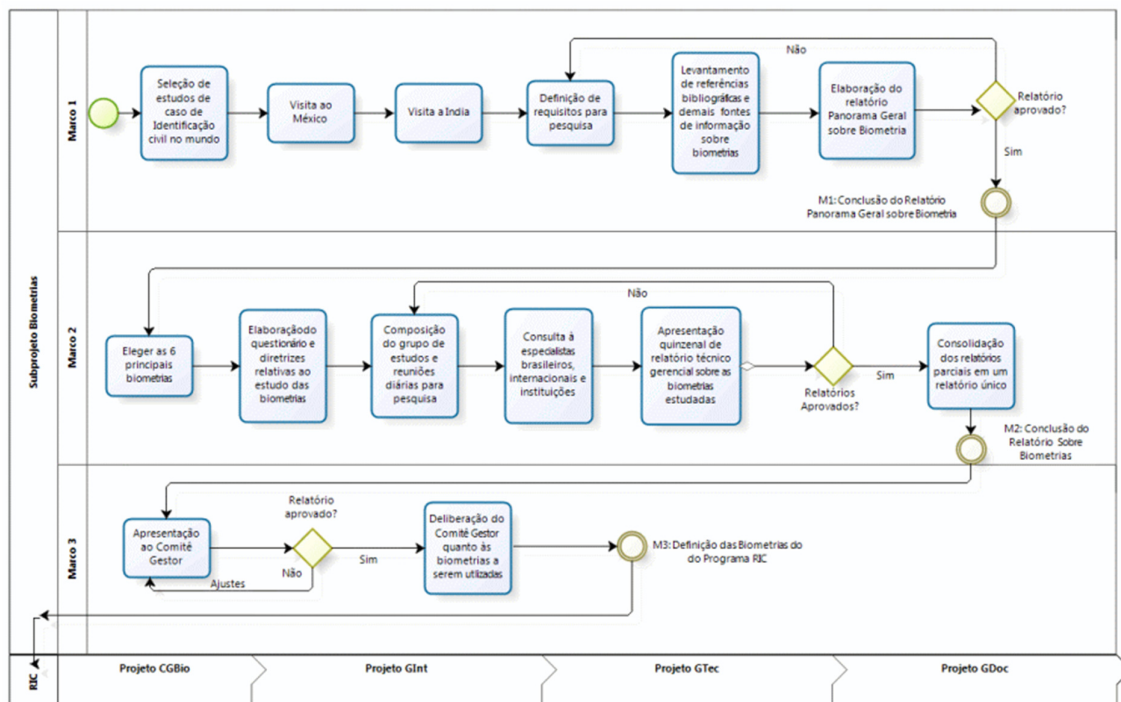


Figura 1 – Fluxograma da Metodologia de Trabalho do Grupo de Biometria

A utilização de tecnologias biométricas em sistemas de grande escala possui características próprias, as quais representam uma gama substancial de desafios para sua implantação. Entre as dificuldades desses sistemas com milhões de pessoas está a decisão da modalidade de biometria mais adequada a ser empregada visando o melhor desempenho deste tipo de sistema.

A eleição da biometria a ser utilizada irá depender do ajuste de oito critérios distintos: custo, interoperabilidade, conveniência de uso, segurança, irrevogabilidade da biometria, precisão do sistema, requisitos técnicos e amplitude de aplicação (Ross et al, 2006) e (Jain et al, 2004).

Tendo em vista a melhor compreensão de cada um desses critérios, foram construídos mapas mentais, os quais pretendem simplificar a forma como tais requisitos se apresentam a partir de uma ou outra biometria. Para isso, estes oito critérios foram simplificados em três categorias gerais, a saber, Conveniência de Uso, Requisitos Técnicos e Segurança.

Dentro de Conveniência de Uso estão presentes os custos, a conveniência de uso, a irrevogabilidade da biometria e a amplitude de aplicação. Dentro de Requisitos Técnicos

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.16/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

estão a precisão do sistema, a interoperabilidade e os requisitos técnicos. E, por último, a categoria Segurança que abrange apenas a segurança.

Ainda vale ressaltar a adoção de sistemas biométricos em outros países, pois servem como experiências fundamentais para o aprendizado de como a tecnologia biométrica pode ser incorporada pela identificação civil. Desta forma, o mapa mental também tenta representar o número de países que adotaram determinada solução biométrica. Adicionalmente, buscou-se também elencar os principais fabricantes em nível internacional e nacional para cada biometria, porém, considerando aplicações em larga escala.

A apresentação dos mapas mentais das biometrias estudadas, anexo ao presente relatório (ANEXO I – MAPAS MENTAIS), tem o objetivo de facilitar a avaliação da adequabilidade de aplicação da referida biometria para o Programa Brasileiro RIC, considerando todos os aspectos acima referidos por meio da utilização visual de cores, sendo a cor verde uma avaliação positiva, cor amarela valoração média e cor vermelha como avaliação baixa. Critérios não coloridos foram descritos com objetivo de auxiliar o entendimento do mapa mental.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.17/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

2 NOÇÕES SOBRE DESEMPENHO DE SISTEMAS BIOMÉTRICOS

2.1 Introdução

A comparação entre dois modelos biométricos depois da extração das características (*templates*) é a parte do processo mais dependente do fornecedor e baseia-se num algoritmo de correspondência (*matching algorithm*) (Gunter, 2013).

A propriedade comum de todos os algoritmos utilizados, independente do fornecedor, é o fato de que eles determinam uma pontuação de semelhança entre, por exemplo, duas impressões digitais a serem comparadas. Dadas as inevitáveis “não-semelhanças” entre amostras da biometria da mesma pessoa, essa pontuação ou nota (*score*) é uma medida estatística para a avaliação de duas amostras originadas da mesma pessoa, apesar de conter elementos distintos.

Para um determinado limite de pontuação, duas amostras de biometria são correspondentes se a pontuação tem, no mínimo, o valor desse limiar (*threshold*). Se a pontuação for menor que esse limiar, as duas amostras da biometria não se correspondem.

Na Tabela 1 são apresentadas algumas definições que são usadas neste documento.

Tabela 1 – Definições utilizadas no documento

Nome	Descrição
Usuário	Pessoa que se submete ao processamento pelo sistema biométrico;
Traço (<i>trait</i>)	Propriedade biométrica avaliada (e.g., impressão digital, imagem da íris, veias da mão);
Amostra	Aquisição única de um traço do usuário;
Usuário genuíno	Usuário cuja identidade corresponde à identidade declarada;
Usuário impostor	Usuário cuja identidade não corresponde à identidade declarada;
Modelo (<i>template</i>)	Conjunto de características essenciais (<i>features</i>) extraídas da

	amostra (ex. minúcias de uma impressão digital);
Equiparador (<i>matcher</i>)	Algoritmo que compara o modelo extraído da amostra com o modelo do gabarito guardado no sistema;
Nota (<i>score</i>)	Número atribuído pelo equiparador a uma amostra, que representa o seu grau de semelhança (ou dissemelhança) com o gabarito, que pode ser guardado no banco de dados do sistema ou em um dispositivo fornecido pelo usuário;
Sistema multimodal (ou multi-traço)	Sistema biométrico que utiliza informação de traços diferentes (ex. impressão digital e imagem de íris);

Neste contexto, é importante também definir verificação (ou autenticação) e identificação, conforme (Dessimoz et al, 2007), como segue.

A **verificação**, também chamada busca um para um (1:1), é a reivindicação de identidade de um usuário, fazendo com que os dados biométricos apresentados sejam comparados com o modelo guardado no banco de dados. Assim, os dados biométricos são adquiridos, pré-processados, transformados em características, e pós-processados, antes de serem comparados com o modelo guardado e a pontuação resultante será comparada com o limiar armazenado calculado ou um valor genérico de limiar.

Na **identificação**, também chamada busca um para “n” (1:n), é feita uma busca no banco de dados de modelos dos usuários para o modelo mais provável do dado biométrico de entrada. Assim, a informação biométrica é adquirida, pré-processada, transformada em características, e pós-processada, antes de ser comparada com todos os modelos de usuários de interesse. O modelo de usuário que obtiver a maior pontuação com respeito à comparação é sugerido que seja a fonte do modelo de entrada.

2.2 Valores de Desempenho – Taxas de Erro

O texto apresentado abaixo e seus respectivos conceitos foram extraídos de (Gunter, 2013).

A seleção do limite de “corte”, também chamado “limite de correspondência”, é uma tarefa muito sensível. Esse limite de correspondência determina implicitamente duas

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.19/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

medidas estatísticas, a saber.

Taxa de Falsa Rejeição (FRR): é a probabilidade de que a pontuação computada para duas amostras da biometria provenientes do mesmo indivíduo esteja abaixo do limiar correspondente fixo (e assim é falsamente considerado como um “no match”);

Taxa de Falsa Aceitação (FAR): é a probabilidade de que a pontuação computada para duas amostras da biometria produzidas por diferentes indivíduos esteja acima do limiar correspondente considerado (e, portanto, falsamente considerado como um “match”).

A FRR e a FAR estão inter-relacionadas. Se a escolha do limiar é feita a fim de manter o FRR baixo, ele irá necessariamente aumentar o FAR, e vice-versa.

A relação entre FRR e FAR geralmente caracteriza o comportamento de um algoritmo e é descrito no *Receiver Operating Characteristic (ROC)* (característica de operação do receptor).

Dependendo da aplicação (por exemplo, alta segurança versus alta conveniência para o usuário), o limiar de correspondência pode ser configurado para obter diferentes pares de valores FRR/FAR. Por exemplo, em áreas de alta segurança uma FAR de 0,1% (ou seja, em média, 1 em cada 1000 tentativas o impostor seria aceito) poderia ser considerado apropriado.

Típicos valores considerados “bons” (ou de “alta qualidade”) são os sistemas operacionais com uma FAR de 0,1% e um FRR de 1-7 % (i.e. 1-7 de 100 tentativas de acessos genuínos seria negado).

Um sistema “bom” de dados significa que as amostras de biometria têm sido obtidas com cuidado e metodologia suficiente. Este tipo de definição vaga é um dos principais problemas na implantação de sistemas de grande escala. Fornecedores tendem a apresentar números obtidos com “boas” amostras de dados, enquanto na prática – devido a várias restrições e condições – dados operacionais reais tendem a ser “menos bons”.

De acordo com (Modi, 2011), em seu livro “*Biometrics in Identity Management: Concepts to Applications*”, as características que influenciam no desempenho da biometria são classificadas conforme tabela abaixo.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.20/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Tabela 2 – Fatores que afetam a performance dos sistemas biométricos

Fatores que afetam a performance dos sistemas biométricos	
FATORES	EXEMPLOS/ DESCRIÇÃO
Características da População	Idade, sexo, ocupação, origem étnica
Aplicação	Tempo entre transações, processo de identificação ou verificação, número de tentativas por transação, sistema com supervisão ou sem supervisão
Fisiologia do usuário	Aparência física como altura, calvície, cor dos olhos e da pele, problemas de saúde com a relativos a garganta ou ao clima frio
Interface com o usuário	Interação física ou não física, auditoria ou feedback visual, número de interações para uma transação completa
Influências ambientais	Temperatura, luz ambiente, umidade, chuva, e neve
Sensores de aquisição de dados	Sujeira, residuo, obstrução, formato
Tamanho do banco de dados	Número de indivíduos envolvidos no banco de dados
Referência: Biometrics in Identity Management: Concepts to Applications, Shimon K. Modi	

Outra característica importante é a taxa de erro equivalente (EER), a qual corresponde a pontuação limiar (*score threshold*) para a qual a FAR e a FRR são iguais. Taxas de EER permitem caracterizar o desempenho do sistema com apenas um valor e não com um par deles (FAR e FRR), já que ambos estão implicitamente inclusos no EER.

2.3 Detalhamento das medidas estatísticas – Métricas de Desempenho

Conforme acima mencionado, o desempenho dos sistemas biométricos é medido, qualificado e expresso utilizando-se diferentes taxas.

Durante a fase de inscrição (cadastro) podem aparecer dificuldades de aquisição com algumas pessoas. Tais dificuldades também são quantificadas por meio das taxas como taxa de falha de aquisição (FTA) e taxa de falha de inscrição (FTE) (Dessimoz et al, 2007).

FTA: percentagem de usuários para os quais o sistema não tem a capacidade de apresentar e adquirir uma amostra biométrica utilizável durante a inscrição e as transações. A FTA, portanto, cobre a FTE e a avaliação da qualidade dos modelos. Por

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.21/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

exemplo, a qualidade da imagem de uma impressão digital pode ser avaliada por meio de algoritmos, os quais irão permitir ou não que se recuse a criação de um molde ou a extração de suas características.

FTE: porcentagem de usuários para os quais o sistema não tem a capacidade de gerar um modelo de qualidade suficiente para a inscrição por causa das limitações da tecnologia. A FTE mede a disponibilidade de uma modalidade biométrica.

Segundo (Maltoni et al, 2009), num sistema biométrico totalmente automatizado, os dados biométricos são capturados automaticamente sem supervisão ou assistência humana. Um sistema deste gênero, normalmente utiliza dispositivos que detectam automaticamente a presença de uma característica biométrica. Por exemplo, um scanner de impressões digitais pode esperar em modo de baixo consumo de energia pela aproximação de um dedo, com um algoritmo de detecção de dedo em execução. Quando o algoritmo de detecção de dedo detecta um dedo, o scanner pode mudar para um modo de captura para capturar automaticamente a imagem da impressão digital. Assim, o sistema automatizado de captura biométrica pode produzir dois tipos de erros: falha em detecção, “*Fail to Detect*” (FTD), e falha em captura, “*Fail to Capture*” (FTC).

O erro de falha de detecção (**FTD**) ocorre quando o dedo se aproxima do scanner de impressões digitais, mas o algoritmo falha na detecção da presença do dedo.

A falha na captura (**FTC**) ocorre quando o sistema sabe que está presente um dedo no scanner, mas não consegue capturar uma amostra.

Estas falhas ocorrem quando a imagem capturada é de qualidade muito baixa, por exemplo, se a superfície do leitor está suja ou ainda quando o módulo de captura é utilizado de forma inadequada: como nos casos em que apenas a ponta do dedo é posicionada sobre o scanner ou o dedo é movido através do scanner variando a velocidade e inclinação da aquisição.

Além disso, podem ocorrer erros dos módulos de extração de características, ou seja, depois de capturadas, as amostras biométricas são enviadas para um módulo que vai processar a extração das características. Se a aquisição da imagem for de baixa qualidade, o algoritmo de extração pode não extrair todas as características utilizáveis. Este erro é denominado falha de processamento, “*Failure to Process*” (FTP).

Os três tipos de erro (FTD, FTC e FTP) são comuns a todos os processos, registro, verificação e identificação, desde o módulo de captura ao módulo de extração de

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.22/125
--------------------	---------------------	---	------------

Confidencial.

características. Muitas vezes esses erros são apenas denominados falha de aquisição, “*Failure To Acquire*” (FTA) (Maltoni et al, 2009).

Neste sentido, (Ross et al, 2006) definem que o FTA, também conhecido como FTC, denota a taxa de proporção de vezes que o dispositivo biométrico falha em capturar uma amostra quando a característica biométrica é apresentada a ele. Este tipo de erro geralmente ocorre quando o dispositivo não é capaz de localizar um sinal biométrico suficientemente bom.

Taxas elevadas de FTA podem afetar o rendimento do sistema biométrico, inclusive elevar os índices de insatisfação do utilizador. O aumento da sensibilidade dos módulos de captura e a extração de características podem reduzir o FTA, no entanto poderá também sobrecarregar os módulos subsequentes.

Outros erros comuns incluem erros de criação de *templates*, ou seja, o módulo de criação de *template*, o qual extrai uma característica ou mais das amostras durante o processo de registro e produz um modelo, também pode falhar (Maltoni et al, 2009). Mais uma vez, isso normalmente acontece quando não há informação suficientemente discriminatória presente nos conjuntos de características, por exemplo, uma área demasiado pequena de uma impressão digital ou quando as imagens das impressões digitais são de má qualidade e, conseqüentemente, o conjunto de recursos tem muito ruído.

Desde que o módulo de criação de *template* é usado no processo de registro, a parte mais crítica do processo, o fracasso do módulo de criação de *template* é também conhecido como falha de registro (cadastro), “*Failure to Enroll*” (FTE). Se a falha para se registrar for desativada, então, podem-se criar *templates* de impressões digitais de baixa qualidade, mas esses *templates* ruidosos resultariam em erros correspondentes superiores.

Adicionalmente, podem ocorrer erros dos módulos de comparação, ou seja, o resultado de um módulo de correspondência de uma impressão digital corresponde a um intervalo [0,1], que quantifica a semelhança entre o conjunto de características para reconhecimento e o modelo de registro (Maltoni et al, 2009). Quanto mais próxima a pontuação é de 1, maior a probabilidade de que o sistema reconheça que o conjunto de características fornecido origina-se do mesmo dedo que está no *template* de registro.

A resposta do módulo de decisão baseia-se em um “*threshold*” (“t”). Os pares de

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.23/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

conjunto de características e modelo de geração de pontuação maior ou igual a “t” são inferidos como pares (ou seja, pertencentes ao mesmo dedo). Se os pares de conjunto de características e modelo de geração de pontuação forem menores que “t”, serão inferidos como pares não correspondentes, isto é, pertencentes a diferentes dedos.

O módulo de correspondência, o qual faz a comparação no modo 1:1 (verificação), pode incidir em dois tipos de erros: (i) confundir um conjunto de características e o *template* originados de dois dedos diferentes como sendo do mesmo dedo, esse erro denomina-se de falsa equivalência; e (ii) confundir conjunto de características e *template* do mesmo dedo como sendo de dois dedos diferentes, erro este denominado de falsa não-equivalência.

É importante compreender a diferença entre erros de falsa equivalência e erros de falsa não-equivalência, bem como entre erros de falsa aceitação e erros de falsa rejeição (Maltoni et al, 2009). Os erros de falsa equivalência e de falsa não-equivalência são erros do módulo de correspondência, na comparação de 1:1, enquanto que o modo de falsa aceitação e falsa rejeição são as taxas de erros associados aos processos de verificação e identificação. Na realidade, o seu significado exato depende do tipo de pedido de identidade apresentado pelo utilizador.

Por exemplo, em aplicações em que é reivindicada uma identidade positiva, uma falsa equivalência a partir do módulo de correspondência resulta numa falsa aceitação, na entrada de um impostor no sistema. Ao passo que a falsa não-equivalência, a partir do módulo de correspondência, causa uma falsa rejeição de um genuíno utilizador do sistema.

A noção de falsa “equivalência/não-equivalência” não é dependente da aplicação e, por conseguinte, é mais apropriada que a noção de falsa “aceitação/rejeição”. No entanto, o uso das noções de falsa aceitação, Taxa de Falsa Aceitação, *False Acceptance Rate* (FAR), e falsa rejeição, Taxa de Falsa Rejeição, *False Rejection Rate* (FRR), é mais popular no setor comercial, conforme detalhado abaixo (Maltoni et al, 2009).

Correspondências perfeitas livres de erros nunca são geradas por sistemas (Dessimoz et al, 2007). Além do fato de que a singularidade pode não ser possível, o resultado do processo de inscrição (cadastro) é influenciado por fatores tais como as condições de aquisição e a intravariabilidade das características extraídas da modalidade biométrica.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.24/125
--------------------	---------------------	---	------------

Confidencial.

Como o modelo (*template*) e a característica fisiológica ou comportamental nunca são exatamente iguais, o sistema tem de calcular e quantificar a semelhança entre eles e, então, de acordo com o critério de correspondência (limite adotado), a decisão é tomada pelo sistema. Este resultado pode não estar adequado com a verdade da questão e o sistema pode gerar dois erros de decisão a respeito da requisição de um usuário (modo de verificação), ou seja: Taxa de Falsa Rejeição (FRR) e Taxa de Falsa Aceitação (FAR), muitas vezes chamados de erros de tipo I e II, respectivamente (Dessimoz et al, 2007).

Se nenhuma reclamação é feita (modo de identificação), dois erros de correspondência são gerados, Taxa de Falsa Correspondência (FMR) e Taxa de Falsa Não-Correspondência (FNMR). FNMR mede a robustez, enquanto a FMR mede a distinção de um sistema biométrico. Por conseguinte, temos, novamente, as seguintes definições.

FRR: percentagem de usuários que requisitou uma identidade específica ou o qual foi reivindicado em uma requisição (tal como, “ele está na lista?”), para a qual o sistema, falsamente rejeitou durante o processo de decisão, ou não tem a habilidade total para adquirir os seus dados biométricos (quando for o caso durante a inscrição). Por esse motivo, FRR também abrange os aspectos FTA / FTE fora de inscrição.

FAR: percentagem de usuários que alegou uma identidade específica ou que foi reivindicado em uma requisição (tal como, “ele está numa lista?”), para o qual o sistema os aceitou falsamente para esta identidade alegada durante o processo de decisão (FTA / FTE não deve ter influência aqui).

FNMR: frequência de ocorrência da taxa de não correspondência (ou seja, o modelo apresentado não coincide com aquele da pessoa já inscrita).

FMR: frequência de ocorrência da taxa de correspondência (ou seja, o modelo apresentado coincide com o de outra pessoa já inscrita).

Segundo (Decann, 2013), erros em reconhecimento biométrico clássico são quantificados utilizando-se FMR, FNMR e ROC no cenário da verificação. Já em sistemas abertos, ou seja, no cenário de identificação, são utilizados **FPIR** (taxa de falsa identificação positiva) e **FNIR** (taxa de falsa identificação negativa).

De acordo com (Gelb e Clark, 2013), FAR é frequentemente referido como FNIR e FRR referido como FPIR.

Considerando sistemas biométricos com de-duplicação do banco de dados, ou seja,

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.25/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

com processo de detecção e manutenção de entradas duplicadas associadas ao mesmo indivíduo, podem ocorrer dois outros tipos de erros, **FDD** (falsa de-duplicação) e **FND** (falsa não-duplicação) (Decann, 2013).

FDD: uma amostra que não está no conjunto de dados, incorretamente corresponde a uma identidade no conjunto não-duplicado.

FND: uma amostra que tem uma identidade correspondente, incorretamente não-corresponde a qualquer identidade no conjunto não-duplicado.

Taxa de Erro de Armazenamento (BER) e Taxa de Penetração (PR) também podem ser medidas (Dessimoz et al, 2007). De fato, algumas abordagens algorítmicas dividem os dados em subespaços, a fim de minimizar o número de amostras para comparar, e assim, a duração do processo de comparação. Mas “quanto mais ocorre a partição do banco de dados, menor a taxa de penetração, mas maior a probabilidade de um erro de partição”. Isso impacta na FNMR.

BER: número de pares de modelo (*template*) – amostras (*samples*) correspondentes que o sistema tem colocado em compartimentos diferentes, no que diz respeito ao número de pares avaliados.

PR: média do número de comparações necessárias – sob o regime de compartimentos – entre cada uma das amostras e a base de dados, divididos pelo tamanho deste último.

FRR e FAR são dependentes das FMR, FNMR, FTA, BER e PR.

De acordo com (Dessimoz et al, 2007), se somente uma simples correspondência de sucesso influencia a aceitação, as equações que representam estas dependências são:

$$FAR = PR \times FMR \times (1 - FTA)$$

$$FRR = FTA + (1 - FTA) \times BER + (1 - FTA) \times (1 - BER) \times FNMR$$

Outras taxas que podem ser utilizadas com as duas acima mencionadas são a Taxa de Erro Equivalente (EER) e a Taxa da Metade do Erro Total (HTER).

EER: esta taxa refere-se à definição do limite em que FNMR e FMR (ou FRR e FAR) são iguais. Esta taxa é frequentemente designada como uma medida do resumo do desempenho. Quanto menor o EER maior é a precisão do sistema.

HTER: esta taxa refere-se a metade da adição de FRR e FAR.

Uma maneira de representar graficamente as taxas FNMR e FMR é usar a curva de Equilíbrio do Erro de Detecção (DET). As taxas de erro são plotadas em ambos os eixos e os desempenhos relativos dos vários sistemas de reconhecimento podem ser melhor distinguidos. A Figura 2 apresenta um exemplo de curvas DET e, portanto, as performances de algumas tecnologias biométricas em protocolos de avaliação específicos. Em geral, sistemas cujas curvas DETs são mais próximas à origem apresentam melhor desempenho (ex. Iris na Figura 2).

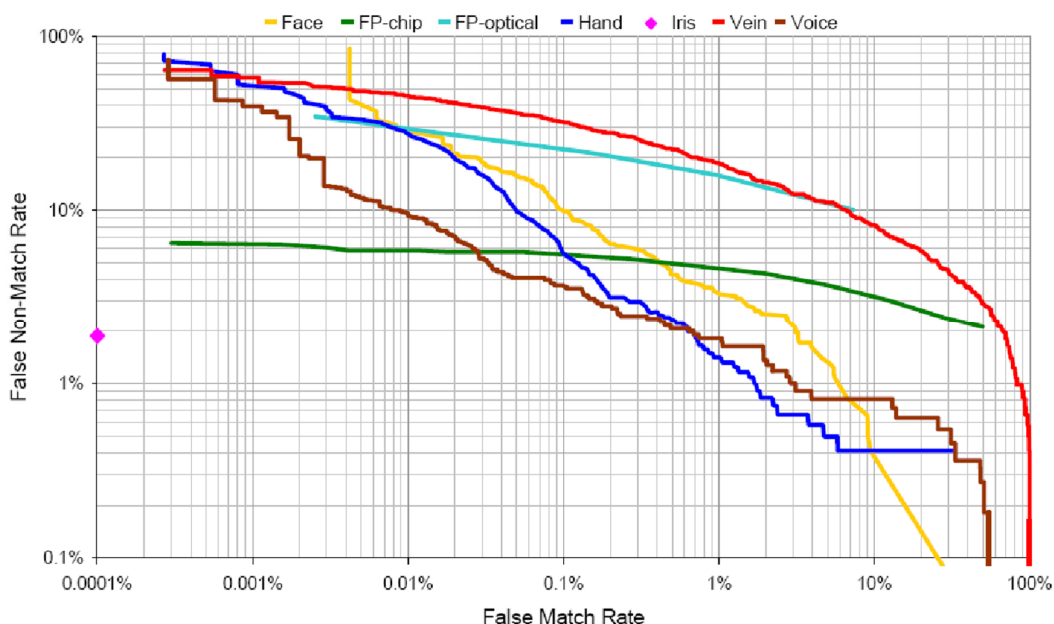


Figura 2 – Curvas DET das principais tecnologias biométricas

Fonte: DESSIMOZ, et al. (2006).

A Figura 2 apresenta alguns números para diferentes modalidades biométricas, as quais são tomadas a partir de diferentes experimentos e, portanto, não devem ser interpretadas como uma comparação direta entre as modalidades biométricas. Na Tabela 3 o desempenho é retratado por meio das taxas FMR e FNMR.

Tabela 3 – Exemplos de desempenho de sistemas biométricos

(apud DESSIMOZ, et al., 2006. Multimodal Biometrics for Identity Documents, State-of-the-Art, Research Report, PFS 841-08.05, version 2.0, June, 2006)

Modalidade	FMR (%)	FNMR (%)	Referências
Face	1	10	PHILLIPS et al., “ <i>Facial recognition vendor test 2002, Evaluation report, March, 2003, available online at http://www.frvt.org/</i> ”
Impressão Digital	0,01	2,54	MAIO et al., “ <i>FVC2004: Third fingerprint verification competition</i> ” in <i>Proceedings of the First International Conference on Biometric Authentication</i> , vol. 3072, 2004 , pp.1-7.
Iris	0,00 129	0,583	<i>International Biometric Group “Independent testing of iris recognition technology”, International Biometric Group, Final Report, NBCHC030114 / 0002, May, 2005.</i>
Assinatura on-line	2,89	2,89	YEUNG et al., “ <i>SVC2004. First International Signature verification competition</i> ”, in <i>Proceedings 2004 Biometric Authentication: First International Conference</i> , (ICBA 2004), Hong Kong, China, July, 2004 , pp. 16-22.
Voz	6	6	REYNOLDS et al., “ <i>The 2004 MIT Lincoln laboratory speaker recognition system</i> ”, in <i>Proceedings IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP 2005)</i> , Philadelphia, USA, March, 2004 , pp.177-180.

Outra maneira de estimar o desempenho de um sistema biométrico é concentrar-se sobre a duração correspondente do processo, chamada de Taxa de Tempo de Correspondência (*Time to Match Rate – TTM*), a saber.

TTM: duração do processo correspondente, desde o final da captura, até a decisão do sistema.

Mais outra medida que pode ditar o desempenho do processo de inscrição (cadastro) é a Taxa de Tempo para a Inscrição (TTE), definida como segue.

TTE: duração do processo de inscrição (cadastro), desde a captura das características do traço fisiológico ou comportamental para a criação do modelo biométrico.

2.4 Principais tipos de erros

Os principais tipos de erros associados a qualquer tipo de desempenho biométrico são: FMR vs. FNMR e FAR vs. FRR. Esses erros são referidos na literatura como pares de erros de desempenho dos algoritmos e do sistema, respectivamente. Eles são relacionados uns com os outros de acordo com as fórmulas abaixo (Gafurov et al, 2010):

$$FAR = FMR \cdot (1 - FTA);$$

$$FRR = FTA + FNMR \cdot (1 - FTA)$$

Nos testes usados na literatura definiu-se FTA usando a fórmula abaixo:

$$FTA = FTC + FTX \cdot (1 - FTC), \text{ em que:}$$

FTC (*Failure to capture*) = falha na captura e

FTX (*Failure to extract*) = falha na extração são abaixo estimados:

$$FTC = \frac{\{(\# \text{ capturas atendidas terminadas}) + (\# \text{ imagens sem qualidade suficiente})\}}{\text{Total \# capturas atendidas}}$$

$$FTX = \frac{(\# \text{ templates não codificados})}{\text{Total \# imagens submetidas ao codificador de template}}$$

("#" = "número de")

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.29/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

É importante observar que o cálculo do FTA incorpora ambos *hardwares* (no FTC) e *software* (no FTX) nas falhas relacionadas.

Neste contexto, cabe salientar que os valores apresentados no relatório de biometria referem-se única e exclusivamente a valores encontrados na literatura vigente, quando possível.

Abaixo é apresentado o desempenho baseado em FAR e FRR das biometrias mais comuns, segundo (Ross et al, 2006). Cabe salientar que quando se compara os dados da Tabela 4 com aqueles da Tabela 3 verifica-se que os erros de FNMR e FMR são apresentados como equivalentes a FRR e FAR, considerando inclusive a mesma referência bibliográfica, ex: face, Tabela 4).

Diante do exposto acima, os dados de desempenho apresentados e avaliados no presente relatório equivalem principalmente a FAR e a FRR.

Tabela 4 – Exemplos de desempenho de sistemas biométricos.

(Fonte: ROSS et al., 2006 – *Handbook of Multibiometrics*)

Biometric Trait	Test	Test Conditions	False Reject Rate	False Accept Rate
Fingerprint	FVC 2004 (Maio et al., 2004)	Exaggerated skin distortion, rotation	2%	2%
Fingerprint	FpVTE 2003 (Wilson et al., 2004)	US Government operational data	0.1%	1%
Face	FRVT 2002 (Phillips et al., 2003)	Varied lighting, outdoor/indoor, time	10%	1%
Voice	NIST 2004 (Przybocki and Martin, 2004)	Text independent, multi-lingual	5-10%	2-5%
Iris	ITIRT 2005 (International Biometric Group, 2005)	Indoor environment, multiple visits	0.99%	0.94%

2.5 De-duplicação

O conceito de de-duplicação refere-se ao processo de examinar, durante o procedimento de cadastramento, se a amostra biométrica que está sendo cadastrada tem alguma amostra correspondente em todo o banco de dados já existente. Desta forma, a amostra é comparada às “N” amostras já cadastradas, uma a uma. Se existe alguma amostra correspondente, o indivíduo não é cadastrado, e, portanto, não recebe uma nova identidade a fim de evitar uma entrada duplicada. Caso não exista amostra correspondente, o usuário é cadastrado de forma correta e um número único é associado à amostra apresentada pelo indivíduo (Decann, 2013).

O processo de de-duplicação é necessário para garantir que todos os indivíduos da população tenham apenas um único número no banco de dados. Por exemplo, uma entrada duplicada pode ser criada intencionalmente por um impostor para futuramente fraudar o sistema e obter algum benefício utilizando a identidade de outro indivíduo.

O processo de de-duplicação vem ganhando notoriedade e atenção nos últimos anos, devido particularmente a programas de identificação civil de grande escala como o caso da Índia, México e Indonésia, em que enormes bases de dados precisam garantir a unicidade dos indivíduos cadastrados.

A de-duplicação também pode ser considerada um processo de identificação, em que é feita uma comparação 1:N. Entretanto, para cada indivíduo que está sendo cadastrado é realizada uma comparação, o que exige alto poder de processamento do sistema. Como exemplo da complexidade dessa operação, a Índia cadastra, diariamente, 1 milhão de indivíduos⁷, os quais são comparados com os 650 milhões já cadastrados⁸, gerando mais de 500 trilhões de comparações por dia⁹.

⁷ <http://pt.slideshare.net/regunathbalasubramanian/aadhaar-at-5thelephantv3>

⁸ <https://portal.uidai.gov.in/uidwebportal/dashboard.do>

⁹ <http://www.youtube.com/watch?v=08sq0y8V1sE>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.31/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

3 ASSINATURA

3.1 INTRODUÇÃO

O uso de assinaturas está imbuído nas sociedades humanas como instrumento para firmar contratos, acordos, tratados e realizar as mais diversas transações. Segundo (Azevedo et al, 2009), sua sistemática baseia-se em um **comportamento** já adquirido e internalizado pelo ser humano, o que o torna ideal para certos tipos de verificação que exigem menor nível de segurança.

Segundo (Sabourn e Genest, 1994), as assinaturas, por representarem um caso especial de manuscrito, podem ser divididas nas categorias, cursivas ou rubricas, estas contendo caracteres especiais, distorcidos ou ainda uma representação simbólica, tais como desenhos estilizados. Neste caso, uma análise não contextual é necessária, pois não existe a interpretação de texto durante a verificação, o que representa outro fator de complexidade.

De acordo com (Cavalcante et al, 2005), a assinatura pode ser entendida como uma sequência lógica de movimentos previamente gravados no cérebro que, praticamente, são impossíveis de serem reproduzidos.

Conforme (Vieira et al, 2010), existem dois modos distintos de reconhecimento: o reconhecimento estático ou *off-line*, e o reconhecimento dinâmico ou *online*.

A verificação estática diz respeito somente ao processamento de imagem: uma pessoa escreve sua assinatura, em papel ou em dispositivo eletrônico, e esta é digitalizada para que haja comparação com amostras previamente inseridas no sistema biométrico.

Segundo (Revett, 2008), tipicamente, o estágio de pré-processamento envolve uma limpeza no fundo da imagem e emprega uma filtragem gaussiana bidimensional, que preserva as bordas da imagem.

O processo de reconhecimento de assinatura manuscrita também é dito como um processo comportamental e não físico, porque se baseia no comportamento da pessoa que irá se autenticar no sistema. Isto quer dizer que não será analisado somente o desenho das letras, que seria incapaz de identificar fotocópias ou falsificações da assinatura, mas principalmente a pressão que a pessoa impõe ao assinar um documento, a velocidade da assinatura e os movimentos impostos durante sua execução.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.32/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

A verificação dinâmica, por sua vez, compreende métodos nos quais ocorre processamento no momento em que a pessoa está escrevendo por meio de um dispositivo eletrônico, como *tablets* ou *PDA's (personal digital assistant)*. Além da imagem, dados como posição em relação aos eixos X e Y, pressão e aceleração são coletados e comparados com entradas anteriores inseridas no sistema, fornecendo resultados mais precisos.

De acordo com (Faundez-Zanuy 2007), a verificação dinâmica é mais vantajosa para ser utilizada como uma forma de autenticação digital, já que alcança um grau de segurança maior quando comparada à verificação estática. Apesar do benefício da segurança, a autenticação biométrica em sistemas informatizados, ainda é pouco popular.

Conforme (Santos, 2004), por mais que alguma semelhança nas assinaturas ou escrita de cada autor possa existir, elementos indicadores de individualidade estarão presentes na sequência de letras de uma palavra: calibre, espaçamento, alinhamento em relação à linha base, inclinação axial, segmentos angulares e segmentos curvilíneos, mínimos gráficos, velocidade, indícios de falsificações (inícios e paradas abruptas, elevação do objeto de escrita, tremor, pressão e correções). As assinaturas genuínas de pessoas em idade avançada ou enfermas podem conter alguns indícios de falsificações em função da baixa permanência de indicadores de individualidade. A presença destes indícios de falsidade (tremor, paradas abruptas, etc.) não significa que a assinatura analisada seja falsa. Tais aspectos podem contribuir na determinação global da autenticidade.

(Costa et al, 2006) definem as etapas para o processo de funcionamento da biometria, conforme transcrito abaixo.

- a. Aquisição;
- b. Pré-processamento: preparação para extração de características através de alinhamento da imagem, limiarização e esqueletização;
- c. Segmentação: particionamento da imagem em células, através de um *grid*, para tratamento do traçado a nível local.
- d. Extração de características (primitivas): nesta etapa são selecionadas as propriedades mais relevantes que representam a assinatura;
- e. Distâncias entre característica: diferença entre os vetores de características

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.33/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

extraídas, usadas na entrada da produção do modelo e no processo de decisão.

- f. Produção de um modelo: um conjunto de referência de assinaturas é gerado para se realizar o processo comparativo;
- g. Processo de decisão: é avaliada a saída do modelo produzido, verificando se a assinatura pertence à mesma classe ou à classes diferentes.

No caso da biometria assinatura, há de se considerar o fator tempo no processo de extração das características. Neste sentido, a análise dinâmica contempla noções de tempo e pressão de escrita, além do espaço bidimensional do papel. Atualmente os dispositivos em uso podem, inclusive, adquirir em intervalos de tempos equidistantes, fluxo de vetores penta-dimensionais.

Por exemplo, um determinado vetor V seria constituído por $V = (x, y, p, qx, qy)$, onde x e y correspondem à posição, p corresponde à força axial exercida pela caneta e qx e qy registram os ângulos da caneta em relação ao plano xy .

O arquivo de assinatura contendo as informações de posição, pressão, azimuth e elevação em função do tempo, em geral apresenta tamanho de aproximadamente 5 a 10 KB, que após comprimido pode ser armazenado em 1 ou 2 KB.

Em geral, as análises de assinaturas dinâmicas são realizadas utilizando-se comparações de medidas de distâncias euclidianas entre as trajetórias de canetas, medidas de correlação regional e reconhecimento temporal-probabilístico, como exemplo as cadeias de Markov ocultas.

Conforme acima descrito, a análise da assinatura dinâmica deve ser baseada na classificação temporal. O conjunto de características que compõem o processo de decisão, constituído de funções temporais, podem ser organizados em quatro grupos, conforme detalhado abaixo, transcrito de (Costa et al, 2006):

- 1. Classificadores probabilistas – Estes métodos são baseados nas distribuições da densidade de probabilidades do conjunto de características genuíno e do conjunto de características em geral. Uma distância entre estas duas distribuições é determinada para fixar o grau de importância de dada característica. A decisão é baseada na distância Euclidiana, computada sobre um conjunto de características.*
- 2. Classificadores elásticos – Esta técnica mais antiga, obscurecida desde o advento das cadeias de Markov ocultas, é baseada na utilização de DTW (Dynamic Time Warping) (Myers e Rabiner, 1981). Esta técnica computa as*

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.34/125
--------------------	---------------------	---	------------

Confidencial.

distâncias temporais mínimas entre um vetor de entrada e os vetores-modelo. Existem diferenças de tempo não-lineares entre as características das assinaturas produzidas pela mesma pessoa. O objetivo é encontrar o alinhamento temporal ótimo entre a assinatura de referência e a assinatura sob verificação.

3. Redes neurais – Esta ferramenta de Inteligência Artificial tem sido explorada para a verificação dinâmica de assinaturas, mas o desempenho registrado tem sido inferior aos outros métodos.

4. Cadeias de Markov ocultas – Cadeias de Markov ocultas (HMM—Hidden Markov Models) são o meio mais popular de classificação temporal, com aplicações em áreas como reconhecimento de discurso, escrita e gesticulação. Informalmente, uma cadeia de Markov oculta é uma variante de uma máquina de estados finita e não-determinística, onde os estados e transições possuem associações probabilísticas (Rabiner e Juang, 1986). Inspirada pelo sucesso da aplicação de HMMs ao reconhecimento de caracteres, este agora é o modelo com melhor desempenho na verificação de assinatura. A vantagem para esta tarefa advém da possibilidade de aceitar variabilidade, ao mesmo tempo em que se captura características individuais da assinatura.

Várias empresas atuam na fabricação de *pads* e *softwares* para coleta e armazenamento da assinatura, dentre elas estão a Topaz Systems Inc., EPAD, StepOver GmbH e Wacom Company Ltda.

3.2 CARACTERÍSTICAS TÉCNICAS

3.2.1 Universalidade

Em geral, todas as pessoas possuem uma assinatura, principalmente porque é uma das formas mais comuns de se autenticar documentos. O que deve ser considerado para avaliação da universalidade são fatores como a “consistência” e a capacidade de executar a assinatura. Por exemplo, crianças menores de 7 anos, dificilmente, conseguem executar uma assinatura consistente.

Outro fator que degrada a característica está relacionado ao nível cultural da população. Segundo informações (Censo IBGE, 2010) existe cerca de 18 (dezoito) milhões de pessoas analfabetas com idades superiores a dez anos no Brasil. Fato este implica que na época existia aproximadamente 9,0% da população que não possuía a característica biométrica.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.35/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

A característica universalidade é avaliada como baixa (Jain et al, 2004).

3.2.2 Singularidade

Segundo (Rasha, 1994), “assinar não é um processo perfeitamente preciso com dados de características idênticas. A única certeza é que quando duas assinaturas são exatamente idênticas, uma delas é provavelmente uma cópia”.

Apesar da dificuldade em se copiar o comportamento da assinatura, esta biometria é avaliada com baixa por (Jain et al, 2004), face as fragilidades e os recursos tecnológicos existentes que facilitam e possibilitam a sua reprodução.

3.2.3 Permanência

Ao contrário dos métodos biométricos fisiológicos (como impressão digital, reconhecimento facial, reconhecimento da retina e íris), que sofrem pouca ou nenhuma variação no decorrer da vida de uma pessoa, a assinatura pode sofrer variação com o passar dos anos.

A característica permanência é avaliada como baixa (Jain et al, 2004).

3.2.4 Coletabilidade

A assinatura é acompanhada de um grande legado histórico, trata-se de procedimentos simples e rotineiramente executados pela população e não é invasiva. A coleta pode ser realizada de duas formas: a primeira trabalha com a análise de dados dinâmicos da assinatura (velocidade, aceleração, pressão, etc.), obtidos quando a assinatura é feita num dispositivo capaz de medir o deslocamento da caneta no tempo (normalmente em um *tablet*). A segunda utiliza a informação estática da assinatura, representada por sua imagem, a fim de serem extraídas suas primitivas (entendidas essas como características capazes de representá-la com unicidade) para posterior comparação.

A característica coletabilidade recebe avaliação alta (Jain et al, 2004).

3.2.5 Desempenho

De acordo com (Costa et al, 2006), ainda se justifica o uso da assinatura nas práticas negociais, pois embora não seja uma das soluções biométricas mais seguras, trata-se de um método para verificação da identidade de uma pessoa.

Na busca 1:1 (verificação), esta tecnologia pode ser utilizada. No entanto a mesma não é eficiente na busca 1:N (identificação).

Algumas pesquisas vêm sendo desenvolvidas, por exemplo, um protótipo de sistema de autenticação baseado em assinaturas dinâmicas foi construído na UNISINOS usando redes neurais do tipo *cascade-correlation* como mecanismo de comparação, relatando bons resultados de precisão, com um ponto de operação (FAR, FRR) estimado em (2,6%, 3,6%) (Heinen e Osorio, 2004).

Segundo um trabalho de pesquisa realizado por (Jain et al, 2002), foi possível atingir uma Taxa de Falsa Rejeição de aproximadamente 2,8% e uma Taxa de Falsa Aceitação de 1,6%, para uma população de 102 pessoas.

Um ponto que compromete a característica é a alta variabilidade. Existem, ainda, muitas pessoas com assinaturas inconsistentes. Diante disto, os sistemas podem necessitar de configuração personalizada por usuário (ex. limiares de decisão).

Segundo (Jain et al, 2004), essa característica é avaliada como baixa.

3.2.6 Aceitabilidade

A assinatura ainda é um dos modos mais aceitos na autenticação da identidade. Esta possibilidade leva a biometria de assinatura a diversos mercados e aplicações, desde a vinculação legal de documentos à checagem de títulos, gerenciamento de documentos e computação com base em caneta eletrônica (*pen-based computing*).

Essa característica é avaliada como alta (Jain et al, 2004).

3.2.7 Resistência à fraude

As assinaturas não genuínas, ou falsificações, são classificadas por (Justino, 2001) em três categorias: simples, habilidosa e aleatória. Na simples, o falsificador escreve o nome do autor, que pode ser semelhante ou não ao original. Na servil, também chamada

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.37/125
--------------------	---------------------	---	------------

Confidencial.

simulada ou habilidosa, o falsificador simula uma assinatura genuína usando um modelo como referência, tentando chegar o mais próximo possível de seu traçado original. Finalmente, na aleatória, o falsificador inventa uma assinatura ou utiliza a sua própria, a qual não possui semelhanças com a genuína.

De acordo com (Sabourn e Genest, 1994), dadas duas classes c_1 , representando a classe de assinaturas genuínas de um autor e c_2 , representando a classe de assinaturas não genuínas, o desafio é basicamente separá-las.

Quando falsificações, principalmente simuladas, são submetidas ao sistema, a complexidade aumenta. Caso seja possível definir um limiar de decisão, a classificação consistirá em determinar em qual lado do limite qualquer novo dado deve ser alocado. A função matemática de tal limite de decisão é uma função discriminante, sendo que achá-la geralmente não é trivial. Devido a isto, em um processo de aprendizagem, algumas amostras de falsificações são identificadas erroneamente como pertencendo à classe c_1 , o que pode acontecer até mesmo com amostras de falsificações simples.

Essa característica é avaliada como baixa por (Jain et al, 2004).

3.3 ESTIMATIVA DE CUSTO

De acordo com (Heinen e Osorio, 2004), o *hardware* necessário a coleta da assinatura tem um custo aproximado entre U\$ 25,00 e U\$ 100,00.

Segundo (Vigliazi, 2006), existem no Brasil dois *softwares* que são muito usados (considerando aplicações para verificação em menor escala): o SignPlus da SoftPro e o GetBioSign da Getronics, sendo que as duas empresas possuem a solução completa de *hardware* e *software*.

Na SignPlus, uma solução de *hardware* e *software* customizado para a criação de um ponto de acesso para o reconhecimento de assinatura custa aproximadamente US\$ 500¹⁰.

Diante da bibliografia existente não foi possível obter informações de custos relativos ao processamento de sistemas, infraestrutura para armazenagem de dados, controle e auditoria das informações.

¹⁰ http://www.ensino.eb.br/artigos/artigo_biometria.pdf

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.38/125
--------------------	---------------------	---	------------

Confidencial.

3.4 CARACTERÍSTICAS DA COLETA

3.4.1 Idade inicial

A idade inicial para coleta da biometria está vinculada diretamente ao nível cultural do cidadão. No segundo ano do ensino fundamental, aos sete anos, o aluno começa a ter discernimento para empreender a assinatura completa de seu nome ou que a represente.

3.4.2 Tamanho do arquivo gerado

O *template* da assinatura (cifrado) possui um tamanho de 1000 a 3000 bytes. Isso se deve a variedade e a quantidade de dados que são necessários para o reconhecimento automatizado da assinatura.

Segundo o trabalho realizado por (Cavalcante et al, 2005), o tamanho do arquivo gerado pela coleta é de 1 KB.

3.4.3 Tempo de coleta

O tempo para coleta está inteiramente interligado ao nível cultural do cidadão, por conseguinte, quanto menor o nível cultural, maior o tempo para coleta da biometria. Implicando numa grande variação.

Foram coletadas amostras de assinaturas de pessoas com nível cultural baixo, de forma cursiva, e de nível cultural elevado, que consumiram um tempo de coleta aproximado entre 142,8 segundos e 3,75 segundos, respectivamente.

3.5 ALGORITMOS DE RECONHECIMENTO

Segundo (Azevedo, 2011), alguns dos algoritmos de reconhecimento mais utilizados são: DTW (*Dynamic Time Warping*), FastDTW e Programação Dinâmica (PD).

De acordo com Costa et al. (2006), resultados da primeira competição internacional de verificação em relação a assinaturas dinâmicas (SVC 2004) relatam taxas de EER entre 2,89% e 16,34% para o melhor e pior algoritmo, respectivamente. No site da competição estão disponíveis arquivos de assinatura adquiridos de 40 usuários, sendo

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.39/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

que cada um forneceu 20 assinaturas.

Segundo (Yeung et al, 2004), existem assinaturas forjadas para cada uma genuína, as quais podem ter sido feitas por falsários que tiveram acesso à impostação da assinatura original. Os arquivos com dados da assinatura possuem informações sobre posição, pressão, azimuth, elevação, registro de caneta em contato e registro de tempo.

3.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Excetuando-se a influência do índice de analfabetismo, que em 2010 representava aproximadamente dezoito milhões de brasileiros, ou seja, 9% da população (Censo IBGE, 2010), acredita-se que as peculiaridades do trabalho e da cultura do brasileiro não interfiram nesta biometria.

3.7 UTILIZAÇÃO EM OUTROS PAÍSES

Não se tem conhecimento do emprego em outros países do reconhecimento automático da assinatura para sistemas de identificação em larga escala.

3.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

Esta biometria não é indicada para identificação (1:N), devido a imprecisão, aos fatores comportamentais e variação na permanência de sua amostra.

Para pequenos grupos pode ser utilizada na verificação (1:1), justificando-se o uso nas práticas negociais, pois se trata de um método, de fato, para verificação da identidade de uma pessoa.

3.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

Embora a assinatura seja uma biometria possível de ser utilizada na verificação (1:1) e em programas de pequena escala, as suas características (universalidade, permanência, desempenho, resistência à fraude) inviabilizam a sua recomendação como biometria primária ou mesmo complementar no Programa RIC.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.40/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Contudo, diante da existência de um vasto legado documental e cultural, sugere-se a manutenção da assinatura convencional nos casos em que as outras biometrias primárias e complementares não possam ser utilizadas.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.41/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

4 FACE

4.1 INTRODUÇÃO

O reconhecimento facial é um método não-invasivo e os atributos faciais são provavelmente as características biométricas mais comuns usadas por seres humanos para reconhecer uma ou outra pessoa. As abordagens mais populares para o reconhecimento facial são com base em: (i) a localização e forma de atributos faciais, tais como os olhos, sobrancelhas, nariz, lábios e queixo e suas relações espaciais (*feature-based method*), e (ii) a análise global (*holistic method*) da imagem do rosto que representa uma face de uma combinação ponderada de um número de faces canônicas (imagem rebatida em eixos) (Jain e Li, 2005).

Embora o desempenho de autenticação dos sistemas de reconhecimento de face disponíveis comercialmente seja razoável (Phillips et al, 2003), estes sistemas impõem uma série de restrições sobre como as imagens faciais são obtidas, muitas vezes, necessitando de um fundo fixo e simples, com iluminação controlada, normalmente sob a supervisão de um operador devidamente capacitado.

Estes sistemas também têm dificuldade de comparar as imagens capturadas a partir de um mesmo rosto obtido de dois pontos de vista diferentes, sob diferentes condições de iluminação e em diferentes tempos, principalmente em relação aos sistemas 2D.

De forma geral, é questionável se o próprio rosto (em função da permanência, mudanças estéticas, singularidade, etc.), sem qualquer informação contextual, é uma base suficiente para reconhecer uma pessoa, de forma automatizada, a partir de um grande número de identidades com um nível extremamente elevado de confiança.

Para que um sistema de reconhecimento facial funcione bem, na prática, deve-se automaticamente (i) detectar se uma face está presente na imagem adquirida; (ii) localizar o rosto se houver um; e (iii) reconhecer a face a partir de um ponto de vista geral (isto é, a partir de qualquer posição).

O reconhecimento facial é um problema de reconhecimento de padrões visuais. Considera-se a face como um objeto tridimensional sujeito a iluminação variável, pose, expressão e assim por diante, e deve ser identificado com base na sua imagem bidimensional (podem também ser usadas imagens tridimensionais, por exemplo, obtidas a partir de laser).

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.42/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

4.1.1 Etapas do processo de reconhecimento

Um sistema de reconhecimento de face geralmente consiste de quatro módulos: detecção, alinhamento, extração de características e comparação, em que a localização e normalização (detecção da face e alinhamento) são etapas de processamento anteriores às de reconhecimento facial (extração de características facial e comparação), conforme ilustra a Figura 3.

A **detecção** facial separa as áreas da face dos objetos de fundo. No caso do vídeo, as faces detectadas devem ser rastreadas usando um componente de rastreamento facial.

O **alinhamento** da face tem como objetivo obter uma localização mais precisa e normalização de rostos quando a detecção facial fornece estimativas imprecisas do local e escala de cada rosto detectado. Componentes faciais, tais como olhos, nariz e boca e contorno facial, ficam localizados; e com base nos pontos de localização, a imagem facial é normalizada em relação às propriedades geométricas, tais como tamanho e pose, usando transformações geométricas ou morfológicas. Em geral, a face é normalizada em relação às propriedades fotométricas tais como iluminação e escala de cinzas.

Depois que a imagem facial é normalizada geometricamente e fotométricamente, a **extração de características** é realizada para fornecer informações eficazes que serão úteis para se distinguir entre os rostos de diferentes pessoas e estáveis em relação às variações geométricas e fotométricas.

Para o processo de **comparação**, o vetor de características extraídas da face é comparado com os *templates* das faces já inscritos no banco de dados; o sistema exibe a identidade do rosto quando for encontrada uma correspondência com suficiente confiança ou indica falha no reconhecimento da face.

Resultados de reconhecimento facial dependem fortemente das características que são extraídas para representar o padrão da face e dos métodos de classificação usados para diferenciar as faces, já que a localização e normalização são a base para a extração de características eficazes. Estes problemas podem ser analisados do ponto de vista de subespaços da face ou seus múltiplos, conforme figura a seguir:

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.43/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

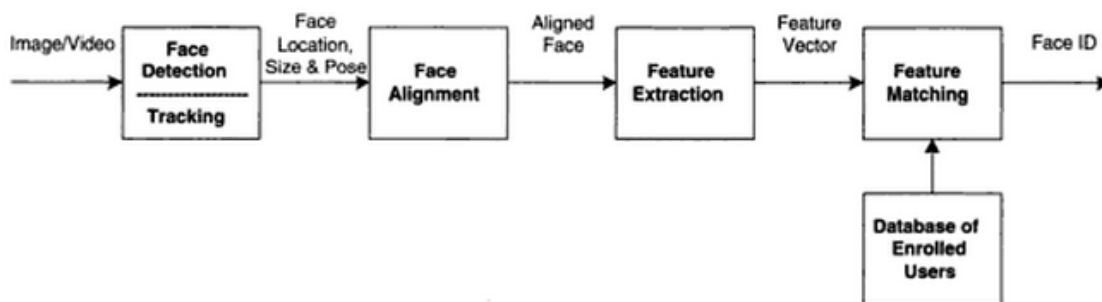


Figura 3 – Fluxograma do processo de reconhecimento facial

(Fonte: STAN Z. Li, ANIL K. Jain, *Handbook of Face Recognition*, 2004)

4.2 CARACTERÍSTICAS TÉCNICAS

4.2.1 Universalidade

A característica universalidade para a biometria face é considerada um dos seus pontos fortes, pois praticamente todo ser humano apresenta uma face que pode ser reconhecida por sistemas automatizados. Essa característica é avaliada como alta por (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006) – nota 5.

4.2.2 Singularidade

Neste quesito a biometria face apresenta um de seus maiores problemas em função da similaridade entre pessoas. A característica singularidade é avaliada como baixa – nota 0. ((Klokova, 2010), ((Jain et al, 2004) e ((Moraes, 2006).

4.2.3 Permanência

Durante as diferentes etapas da vida de um ser humano como a infância, adolescência, fase adulta e terceira idade, ocorrem várias modificações dos pontos nodais da face, o que resulta em uma biometria com baixa permanência. Outro fator a ser levado em conta é a possibilidade de mutação através de acidentes ou procedimentos como cirurgias plásticas e utilização de produtos de rejuvenescimento. Tais fatos impõem atualizações cadastrais em várias etapas da vida, o que causa impacto no custo do sistema. A característica permanência é avaliada como mediana – nota 3. (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.44/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

4.2.4 Coletabilidade

Esse traço biométrico é fácil de ser adquirido sem a cooperação do indivíduo e, portanto, a característica coletabilidade recebe avaliação alta – nota 5 (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

No entanto, para a identificação civil, em um projeto de larga escala, é necessária a coleta da biometria face em ambiente controlado (pose frontal, distribuição uniforme de iluminação, expressão, oclusão de pontos nodais, uso de acessórios), seguindo normas e padrões internacionais.

4.2.5 Desempenho

O desempenho dos sistemas de reconhecimento facial é muito dependente do tipo de aplicação. Existem competições de avaliação a fim de avaliar o desempenho dos algoritmos. Em relação aos sistemas de reconhecimento facial 2D, um dos estudos de maior prestígio sobre a precisão dos algoritmos de reconhecimento facial é elaborado pelo Instituto Nacional de Padrões e Tecnologia (*NIST – National Institute of Standards and Technology*) (Grother et al, 2010). O fato de ser um estudo feito por uma agência independente traz bastante credibilidade aos resultados. Da informação disponibilizada, pode-se concluir que os algoritmos estão muito mais precisos, já que em 2010, conseguiu-se uma Taxa de Falsa Aceitação (FAR) de apenas 0,003%, comparado com o valor de 0,79% obtido no ano de 1993. A população considerada para estes testes foi de 1,6 milhões de indivíduos e foram avaliados algoritmos de empresas como NEC, Sagem Morpho, entre outras.

Nas Tabela 5 e Tabela 6 encontram-se resultados da FRVT (*Face Recognition Vendor Test*) realizados em 2002 e 2006:

Tabela 5 – FRVT2002: Avaliação comercial do sistema de reconhecimento facial 2D.

FRR	FAR
10%	1%
18%	0.1%
Obs.: Iluminação externa: taxas de reconhecimento cai mais que 40% para imagens tomadas externamente	

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.45/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Tabela 6 – FRVT2006: Avaliação comercial dos sistemas de reconhecimento facial 2D e 3D.

(Fonte: *Face Recognition* – A tutorial, Filareti Tsalakanidou – FRGC presentation in Biometrics Consortium 2005 – <http://www.iti.gr/iti/files/document/seminars/FR2.pdf>)

Sistema	FRR	FAR
2D	2-5%	0.1%
3D	0.5-3%	0.1%

Essa característica é avaliada como baixa – nota 0 (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

4.2.6 Aceitabilidade

A face é uma das biometrias mais aceitáveis e conhecidas no mundo, por se tratar de uma das formas mais comuns de identificação, que se baseia nos traços do rosto das pessoas. Os seres humanos têm grande facilidade em reconhecer o rosto das pessoas sem nenhum problema. Essa característica é avaliada como alta– nota 5 ((Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

4.2.7 Resistência à fraude

A face é uma das biometrias mais fáceis de serem fraudadas. Vários métodos são empregados no momento da falsificação da autenticidade de um indivíduo. Os três principais tipos de fraude são a utilização de maquiagem, a utilização de máscaras e a realização de cirurgias plásticas, sendo as duas últimas as mais eficazes. Outro tipo de fraude possível no caso da face é quando há o reconhecimento das características da face em irmãos gêmeos (Geradts e Sommer, 2006). Essa característica é avaliada como baixa – nota 0 (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

4.3 ESTIMATIVA DE CUSTO

De acordo com uma licitação recente de equipamentos biométricos, para uma que amostra de 2 milhões de pessoas, tem-se:

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.46/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Tabela 7 – Estimativa do custo da face.

Fornecedor	Sistema Rec. Facial (R\$)	Custo Unitário (R\$)
1	2.948.880,00	1,47
2	4.151.627,52	2,08
MÉDIA	3.550.253,76	1,78

Observação: nos valores mencionados estão considerados os custos de infraestrutura que compreendem os equipamentos, dispositivos, acessórios e *software*.

Diante dos valores acima (utilizando-se a média dos valores totais) e para a capacidade de 2 milhões de pessoas, o custo unitário de implantação do sistema por pessoa é de R\$ 1,78.

Considerando-se o custo por face cadastrada de R\$1,78, o custo total para 200 milhões de pessoas é de aproximadamente 355 milhões de reais (R\$ 355.025.376,00). Entretanto, esse custo não deve ser considerado como custo final de aquisição, processamento e reconhecimento da face. Trata-se apenas de uma estimativa de custo.

Os principais fabricantes de equipamentos de reconhecimento facial no mercado são¹¹ NEC, Aware, Anviz Global, ZKTeco, FaceFirst, Cross Match Technologies, Smartmatic, MorphoTrak, Cognitec.

4.4 CARACTERÍSTICAS DA COLETA

4.4.1 Idade inicial

Não há na bibliografia consultada, idade recomendada para coleta desta biometria. Isto está diretamente relacionado à baixa permanência da biometria, fazendo-se necessária a coleta constante com a finalidade de atualização cadastral.

4.4.2 Tamanho do arquivo gerado

Segundo (Camp, 2007), o tamanho médio do *template* de reconhecimento facial varia de 83 a 1000 bytes.

¹¹ <http://findbiometrics.com/solutions/facial-recognition/>

4.4.3 Tempo de coleta

De acordo com o programa de identificação civil indiano (UIDAI), o tempo de coleta da biometria facial é de 34 (trinta e quatro) segundos (UIDAI 2012b).

4.5 ALGORITMOS DE RECONHECIMENTO

A avaliação de quão bom um algoritmo é para realizar a identificação de uma determinada biometria depende de qual característica se está analisando: EER, FRR, FAR, velocidade de comparação, velocidade de cadastramento, tamanho do banco de dados, dentre outras.

Além disso, ano após ano, são realizadas competições para se verificar quais algoritmos apresentam melhores resultados, como é o caso da FRGC (*Face Recognition Grand Challenge*) e FRVT (*Face Recognition Vendor Test*). Os valores das Taxas de Falsa Aceitação e Falsa Rejeição estão na seção de desempenho do sistema.

4.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Como já informado anteriormente, a universalidade desta biometria é elevada, inclusive na população brasileira. Acredita-se que não haja influências restritivas do trabalho ou da cultura do brasileiro em relação à utilização da face como biometria para identificação.

4.7 UTILIZAÇÃO EM OUTROS PAÍSES

Embora a maioria dos países já utilizem a biometria facial para reconhecimento, não há registro de utilização da face como biometria para identificação civil automatizada e em larga escala.

4.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

Esta biometria não é apropriada para o processo de identificação (1:N) em virtude da baixa resistência à fraude, da permanência mediana e também ao baixo desempenho do sistema de reconhecimento.

Embora esta biometria possa ser utilizada para verificação (1:1), seu uso em sistemas de larga escala pode acarretar elevados custos com armazenamento, processamento e

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.48/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

atualização.

4.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

Em virtude da baixa singularidade, baixa resistência à fraude, baixo desempenho e tamanho e tempo de processamento do número de pontos nodais necessários para a individualização, e considerando a larga escala do projeto em questão (200 milhões), a biometria facial não é aconselhável para a identificação civil, portanto, não é recomendada para o Programa RIC como biometria de identificação (1:N).

No entanto, em função da tradicional utilização da imagem facial das pessoas na autenticação visual, esta biometria pode vir a ser utilizada como biometria complementar.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.49/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

5 IMPRESSÃO DIGITAL

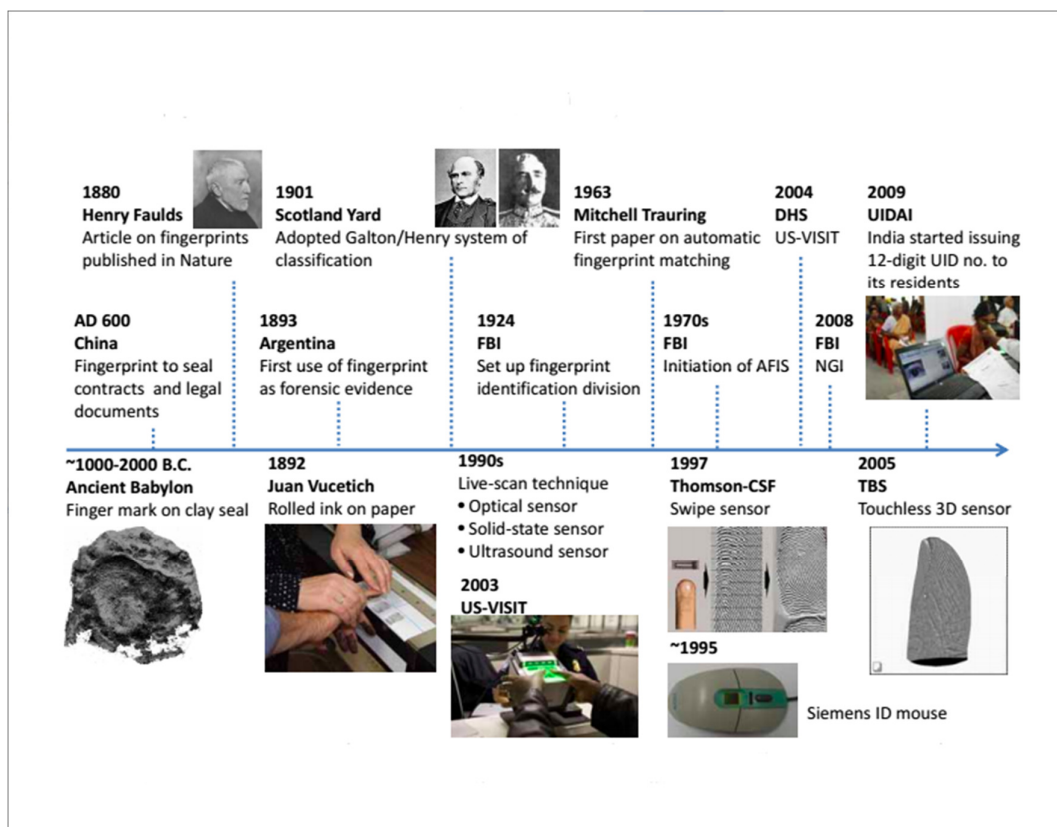


Figura 4 – Histórico do reconhecimento da impressão digital

Fonte: *50 Years of biometrics research*¹².

5.1 INTRODUÇÃO

Serão descritas, a seguir, as principais características da biometria impressão digital com o objetivo de possibilitar a comparação com as demais biometrias estudadas, a fim de embasar a tomada de decisão para a escolha das biometrias que irão compor o Programa de Identificação Civil brasileiro.

A Datiloscopia, do grego “*DAKTYLOS*” que significa dedos e “*SKOPEIN*” que significa examinar, é um método de identificação baseado no reconhecimento das impressões digitais. É considerada uma das tecnologias biométricas mais prática, segura e econômica

¹²

http://biometrics.cse.msu.edu/Presentations/AnilJain_50YearsBiometricsResearch_SolvedUnsolvedUnexplored_ICB13.pdf

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.50/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

que existe.

Para o reconhecimento automatizado das impressões digitais é utilizado, desde a década de 80, o Sistema Automatizado de Identificação de Impressões Digitais (AFIS) para controle de imigração, controle de acesso, porte de armas, transações eletrônicas, controle e gerenciamento de ponto, etc.

I.1 Princípios fundamentais da Datiloscopia

De acordo com a literatura, são quatro os princípios fundamentais que regem a datiloscopia, a saber.

Perenidade: segundo o Manual de Cadastramento biométrico do eleitor brasileiro (ANP e INI, 2009), perenidade é a propriedade dos desenhos papilares se manifestarem definidos e observáveis desde a vida intrauterina até a completa putrefação cadavérica. Desta forma, cada pessoa pode ser classificada por um conjunto de características que permanecem por toda vida.

Imutabilidade: de acordo com a mesma referência (ANP e INI, 2009), é a propriedade dos desenhos papilares de não mudarem sua forma original, desde o seu surgimento até a completa decomposição cadavérica.

Classificabilidade: as figuras papilares podem ser classificadas e medidas quantitativamente para pesquisa e arquivamento.

Variabilidade: é a propriedade dos desenhos papilares em variar de dedo para dedo e de pessoa para pessoa, ou seja, os desenhos papilares não se repetem, garantindo assim a unicidade da referida biometria. Não há possibilidade de se encontrar dois desenhos papilares idênticos, nem mesmo em uma mesma pessoa (ANP e INI, 2009).

Neste sentido, duas impressões digitais só serão consideradas idênticas quando apresentarem, no mínimo, doze pontos característicos com a mesma configuração e que tenham exatamente a mesma localização.

I.2 Pontos Característicos ou Minúcias

Os pontos característicos acima mencionados são também chamados de “minúcias”. Esses pontos característicos ou minúcias são acidentes encontrados nas cristas papilares e são usados para estabelecer a unicidade das impressões digitais. Utilizando-se a

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.51/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

posição e localização dessas minúcias é possível fazer a verificação da impressão digital para estabelecer sua procedência.

Os pontos característicos ou minúcias podem ser qualificados em duas categorias: aspectos básicos e aspectos compostos¹³.

Os aspectos básicos são compostos por figuras comuns extraídas de imagens de impressões digitais e constituídos de cristas finais e bifurcadas, de acordo com a Figura 5. O ponto em que a crista termina abruptamente é definido como crista final, já os pontos de divergência dentro de vales são chamados de cristas bifurcadas.

Os aspectos compostos, formados a partir dos básicos, são constituídos por ilhas, cristas curtas, esporas e cruzamentos, conforme Figura 5. Duas bifurcações conectadas são definidas como ilhas ou lagos, enquanto cristas quebradas ou simplesmente cristas finais muito pequenas são definidas como cristas curtas ou independentes. Esporas são formadas pela junção de bifurcações e cristas finais. Pontes ou cruzamentos são as conexões de duas ou mais bifurcações com um caminho conectado¹⁴.

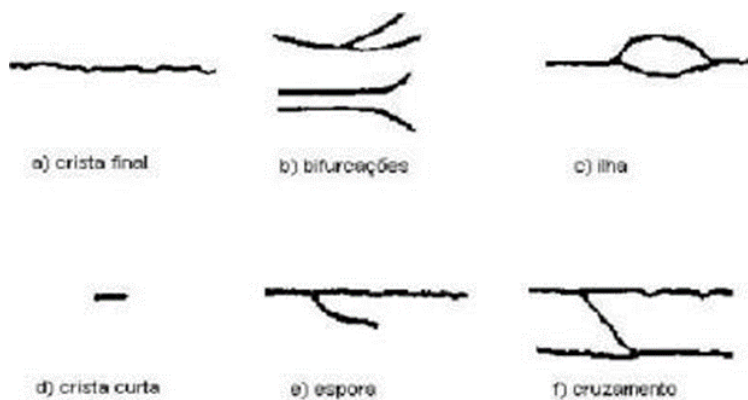


Figura 5 – Tipos de pontos característicos ou minúcias

Fonte: <http://sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/minucias/minucias.html>

1.3 Pontos Singulares

As impressões digitais podem ser classificadas de acordo com pontos singulares, os quais são desenhos digitais com características próprias. São pontos singulares: deltas e

¹³ sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/idigital.htm

¹⁴ sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/idigital.htm

linhas do sistema nuclear (núcleo).

A bifurcação de uma linha simples ou a divergência brusca de duas linhas, as quais estejam em paralelo, formando um triângulo composto pelas cristas papilares, define um delta¹⁵. É o delta que determina a classe da impressão digital, representando o ponto de divergência das linhas dactilares mais internas que tendem a envolver a região nuclear de uma impressão digital (Figura 7).

As impressões digitais que não têm delta, no caso dos arcos planos, possuem somente as linhas basilar e marginal (Figura 7).

Quando a impressão tem um ou dois deltas, é classificada em três sistemas de linhas: nuclear (região central da impressão), basilar (linha que serve de base, abaixo da região nuclear) e marginal (região das características situadas nas margens da impressão) (Figura 6).

Núcleo é um ponto localizado na área central da impressão digital (Figura 6).



Figura 6 – Sistemas de linhas das impressões digitais.

¹⁵ sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/idigital.htm



Figura 7 – Regiões da impressão digital e pontos singulares, marcados em vermelho

Fonte: <http://sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/classes/classes.html>

Os desenhos na forma de delta e linhas do sistema nuclear (núcleo) permitem classificar a impressão digital de acordo com os respectivos pontos singulares, conforme apresentado na Figura 8¹⁶.



Figura 8 – Deltas e linhas utilizados na classificação e verificação das impressões digitais.

Fonte: <http://sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/classverif/classverif.html>

I.4 Classificação de Impressões Digitais

A classificação de impressões digitais pode ser feita de acordo com o número e localização dos pontos singulares. A maioria dos métodos de classificação existentes faz uso da imagem direcional que fornece informações contidas nos padrões de impressões

¹⁶ sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/idigital.htm

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.54/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

digitais e pode ser seguramente calculada em imagens ruidosas, já que para atenuar a influência dos ruídos, basta tomar a média das direções (Figura 9)¹⁷.

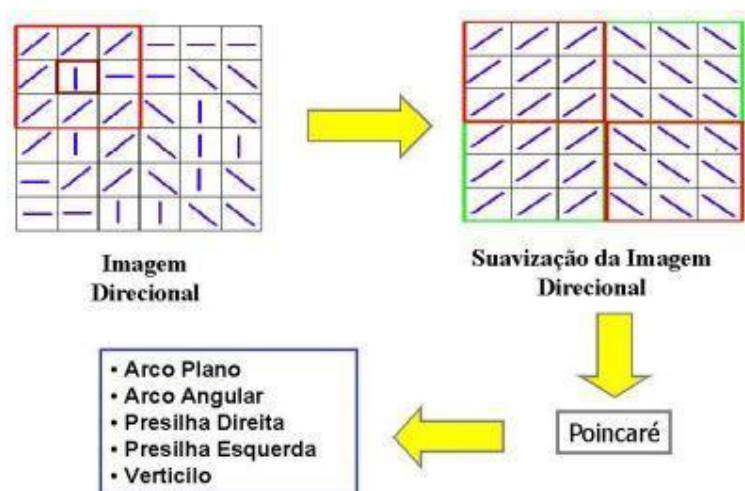


Figura 9 – Exemplo e etapas de transformação da imagem direcional

Fonte: <http://sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/proclassif/proclassif.html>

De acordo com (Costa, 2001), para o cálculo do índice de Poincaré, o pixel na imagem direcional é classificado como: ordinário, núcleo, ou delta.

I.5 Processamento de Impressões Digitais

As características biométricas baseadas em impressão digital correspondem a um padrão geométrico da distribuição de minúcias e são chamadas de *templates*.

Há dois tipos básicos de imagens de impressões digitais: as planares e as completas (também conhecidas como unha a unha ou rolada).

No entanto, segundo o Manual de Cadastramento Biométrico do Eleitor Brasileiro (ANP e INI, 2009), há três modos básicos de capturar as digitais, baseados no contato do dedo: a coleta varrida, a pousada (ou batida) e a rolada.

O texto transcrito a seguir detalha as etapas do processo e foi extraído na íntegra do Manual de Cadastramento Biométrico do Eleitor Brasileiro (ANP e INI, 2009):

As coletas varridas ocorrem frequentemente em dispositivos de segurança portáteis ou móveis, tais como notebooks, celulares, pen drives, fechaduras de

¹⁷ <http://sim.lme.usp.br/linhas/iinteligente/pimagem/idigital/proclassif/proclassif.html>

porta, entre outros. Neste tipo de coleta, as imagens das impressões digitais são reconstruídas a partir de sucessivas fatias de imagens, que são emendadas depois da aquisição de todas as fatias. Como o sensor é bastante pequeno, ele pode ser aplicado em dispositivos móveis e geralmente permitem coletas rápidas. Quando utilizados com sensores térmicos, possibilitam coleta muito robusta, como aquelas em que o sujeito tem as mãos sujas ou até calçadas com luvas cirúrgicas. Porém, ainda não há um sensor desse tipo que consiga capturar uma digital completa.

As coletas pousadas ou batidas são caracterizadas pelo pouso do dedo sobre uma superfície plana, cuja imagem é capturada toda de uma vez. A vantagem destas é a rapidez na coleta. Além disso, é um método barato, pois se utiliza dos primeiros tipos de sensores fabricados em larga escala. Porém, também não permite a coleta de digitais completas (ANP e INI, 2009).

A captura rolada é a única baseada em tecnologia de contato que permite a captura de impressões digitais completas. Para isso, exige uma operação de rolagem do dedo sobre uma superfície plana. A rolagem do dedo gera um conjunto de imagens sucessivas que, logo após a rolagem, são reconstruídas formando uma única imagem. Essa operação requer um tipo de sensor que permita a rolagem, pois o dispositivo deve ser capaz de registrar um conjunto de imagens durante a rolagem. Normalmente, os sensores adequados são capazes de registrar 15 imagens em um segundo e também possuem uma superfície maior para exposição do dedo, para que ele possa ser rolado.

Um dos sensores utilizados no Brasil (TSE) é baseado em uma tecnologia conhecida pela sigla em inglês TIR, que significa Reflectância Interna Total.

O princípio de seu funcionamento é bem simples. O dedo entra em contato com um prisma de vidro que tem uma luz incidindo do outro lado. Esse arranjo óptico fará com que a luz só seja refletida pela superfície do prisma que não é tocada pelas papilas dérmicas (os sulcos), gerando partes claras na imagem formada no CCD. Por outro lado, onde a luz é absorvida, ou seja, nas linhas papilares, as regiões da imagem ficarão escuras.

Para que uma imagem coletada seja útil para a identificação, o computador deverá localizar onde estão todas as minúcias daquela imagem. Para isso, há um conjunto de processamentos computacionais sucessivos que, ao final, resultarão em uma lista das minúcias e suas características. Estes passos são os seguintes: 1) melhoramento e binarização; 2) afinamento ou esqueletonização; 3) extração das minúcias; 4) armazenamento das minúcias, conforme detalhado a seguir.

Melhoramento e binarização

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.56/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

O melhoramento da imagem é um processamento, realizado pelo computador, no qual a imagem é submetida a um tipo de filtro (chamado Filtro de Gabor). Pode-se pensar este filtro como uma ponta de lápis-borracha que percorre cada região da imagem e, por onde passa, consegue reconhecer a orientação das linhas de elevações e então borrar apenas nessa direção. Ele é fundamental para que as minúcias que forem detectadas nas etapas posteriores sejam aquelas que realmente existem no dedo e não aquelas causadas por ruídos da imagem.

As minúcias não são extraídas diretamente da imagem melhorada. É preciso binarizá-la, ou seja, percorrer cada elemento da imagem e decidir se ele será preto ou branco, de acordo com o seu tom de cinza. Por exemplo, se o tom de cinza for mais claro que um índice de cinza desejado, então aquele elemento se tornará branco; caso contrário, será preto. O resultado é uma imagem que mostra as elevações como linhas grossas totalmente pretas e os vales como linhas grossas totalmente brancas. Em alguns dispositivos, as minúcias são extraídas diretamente da imagem binarizada.

Afinamento ou esqueletonização

O afinamento é necessário para a extração de minúcias de forma mais precisa. O afinamento consiste na redução das linhas escuras da imagem até que cheguem à largura de um único elemento (pixel).

Extração de minúcias

As minúcias, ou seja, bifurcações e terminações, precisam ser detectadas para serem extraídas. Por isso, recorre-se à imagem afinada para identificar linhas e, então, buscar nestas linhas as suas extremidades e bifurcações, bem como calcular o ângulo de cada uma dessas extremidades e bifurcações.

Armazenamento das minúcias (*templates*)

Uma minúcia corresponde, portanto, a um ponto localizado na imagem que possui um ângulo. Então, para armazená-las, é preciso apenas construir uma lista de minúcias

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.57/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

contendo suas posições e sua medida de ângulo. Esta lista pode ser armazenada como um arquivo-texto comum e ser gravada em qualquer mídia digital, ocupando muito pouco espaço. Por isso, em cartões de identificação com chip é possível colocar este conjunto de minúcias para identificar o seu portador.

Portanto, para um único dedo, a extração de minúcias gera uma lista que será armazenada como um arquivo.

Finalmente, de acordo com o Manual de Cadastramento Biométrico do Eleitor Brasileiro (ANP e INI, 2009), a comparação biométrica considera a geometria das distribuições das minúcias, ou seja, o número de ângulos e tamanhos de arestas parecidos entre as duas geometrias. Portanto, quanto maior este número, mais parecidas são as impressões digitais em comparação.

5.2 CARACTERÍSTICAS TÉCNICAS

5.2.1 Universalidade

A impressão digital é uma das biometrias mais comuns nas pessoas.

De acordo com várias compilações (tabelas classificatórias de biometrias), a impressão digital é classificada como de universalidade média (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006), (Hong et al, 2005). De acordo com (Moraes, 2006), numa valoração de 0 a 5, o valor expresso para universalidade da impressão digital foi 3.

A valoração média para a universalidade da impressão digital se deve ao fato de que embora a grande maioria das pessoas inerentemente possua digitais desde o momento do nascimento, as mesmas podem ser danificadas ao longo da vida por doenças de pele, perda de dedos, cicatrizes e até mesmo o trabalho rotineiro.

Neste sentido, tanto para ampliar a abrangência da aplicabilidade dessa biometria (população coberta pelo sistema) como a precisão do sistema, estudos desenvolvidos em países como Índia e México recomendam a coleta decadal de impressões digitais, a qual possibilita também a escolha da melhor amostra para ser utilizada no processo comparativo de autenticação.

Considerando as características da população brasileira é importante salientar que cerca de 14,2% tem suas atividades na agricultura, pecuária, produção florestal, pesca e

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.58/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

aquicultura e mais 6,9% têm atividades vinculadas ao serviço doméstico (Censo IBGE, 2010)¹⁸, os quais podem apresentar danos e desgastes nas impressões digitais. Portanto, 21,1% da população brasileira apresentam potencial de desgaste ou dano na impressão digital. Isso representa nos dias de hoje cerca de 42 milhões de pessoas.

Comprometendo a universalidade, existem diversas síndromes em que a pessoa nasce sem as impressões digitais, como o caso da síndrome de Nagali. Além das síndromes, existem as doenças de pele, como a dermatite e epidermólise bolhosa, as quais causam feridas na pele e acometem as digitais. Tem-se também a psoríase, a qual causa vermelhidão e descamação da pele.

5.2.2 Singularidade

Singularidade refere-se a distinção que separa os traços biométricos individualmente a partir de outro. Até gêmeos univitelinos apresentam diferenças nos desenhos das impressões digitais.

Devido às impressões digitais serem únicas para cada pessoa, ou seja, possuírem padrões diferentes para pessoas diferentes, a singularidade dessa biometria é valorada como excelente, recebendo nota máxima - nota 5 (Jain et al, 2004), (Moraes, 2006).

5.2.3 Permanência

O ponto forte da impressão digital é a sua permanência, já que os traços biométricos permanecem inalteráveis durante praticamente todo o ciclo de vida do usuário. No entanto, eventualmente, dependendo da atividade profissional executada, os traços biométricos da impressão digital são alterados, chegando até ao desaparecimento, como em casos de constante utilização de produtos químicos ou de trabalhos manual e rural.

Sob condições de desgastes normais a impressão digital permanecerá inalterada ao longo da vida. Desta forma, é dada a nota máxima a esta característica biométrica (Klokova, 2010), (Jain et al, 2004), (Moraes, 2006) e (Hawthorne, 2009).

5.2.4 Coletabilidade

Coletabilidade refere-se a facilidade de aquisição ou coleta do traço biométrico. A coletabilidade da impressão digital é classificada como média devido a possibilidade de

¹⁸ <http://www.ibge.gov.br/home/presidencia/noticias/imprensa/ppts/00000008473104122012315727483985.pdf>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilizacao no RIC.docx	Pág.59/125
--------------------	---------------------	---	------------

Confidencial.

interferência do operador, do usuário e do sensor, e suas combinações. Embora seja de fácil coleta/aquisição, existe uma alta taxa de erro (5%) mesmo com *softwares* e sensores de qualidade.

A coleta de impressões digitais pode ser feita de modo rolado ou batido. Ressalta-se que a coleta rolada exige maior preparo e treinamento dos operadores para sua correta extração.

Segundo o Comitê sobre Biometria da Índia (UIDAI 2009), testes de campo com 25.000 pessoas (250.000 impressões digitais) sugerem que a qualidade e, conseqüentemente, a precisão dos dados das impressões digitais diminuem vertiginosamente se não for dada a devida atenção ao processo operacional de coleta. Um nível mínimo de formação de operadores envolvidos na coleta das imagens é necessário para a manutenção da qualidade das mesmas.

O Comitê Biométrico Indiano optou pela coleta de impressões apenas de modo pousado em função da menor interferência entre operador e usuário.

Embora a formação das impressões digitais aconteça nos primeiros sete meses de gestação, permanecendo intactas por toda a vida, a União Européia recomenda a sua coleta somente a partir dos 6 anos de idade (Guenter, 2013). Para crianças, os tamanhos das estruturas das impressões digitais mais relevantes (em particular, a distância entre os sulcos) são até um terço menores do que para os adultos.

Segundo (Moraes, 2006), a nota da coletabilidade é 3.

5.2.5 Desempenho

O desempenho da impressão digital é considerado alto.

A comunidade de biometria tem reunido esforços para a avaliação de sistemas de identificação de grande escala. O resultado desses testes é utilizado para importantes tomadas de decisão e é imperativo que as métricas desses estudos de desempenho sejam confiáveis. Por isso, são utilizadas amostras de dados reais obtidas de sistemas de identificação como em fronteiras territoriais, oferecendo uma visão real do desempenho do sistema.

Existem algumas metodologias de avaliação do desempenho de reconhecimento da impressão digital, sendo os mais importantes o FpVTE e FVC.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.60/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

O FpVTE (*Fingerprint Vendor Technology Evaluation*), foi criado pelo NIST para avaliar as características de identificação e verificação de sistemas comerciais para determinação do desempenho de reconhecimento. O resultado deste teste foi publicado em 2003, conforme tabela a seguir. Foram utilizados um total de 393.000 imagens de impressão digital distintas de mais de 34 sistemas diferentes. A principal observação foi de que o desempenho dos sistemas de grande escala pode ser elevado melhorando-se a qualidade da imagem coletada e o número de dedos de um mesmo indivíduo. (FpVTE 2003)

O FVC (*Fingerprint Verification Competition*) foi concebido como uma competição aberta para o julgamento da performance dos algoritmos de reconhecimento de impressão digital. O FVC foi realizado em 2000, 2002, 2004 e 2006 e atraiu participantes da indústria e da academia. No final de cada competição realizada, todos os participantes são ranqueados baseados nas seguintes métricas de performance: Taxa de Falsa Aceitação (FAR), Taxa de Falsa Rejeição (FRR), Taxa de Erro Equivalente (EER), tempo de coleta, tempo de comparação, entre outras. O FVC iniciou uma nova competição, chamada FVC *On Going*, baseada em internet (*WEB-based*), na qual os participantes podem enviar seus algoritmos de reconhecimento (atendendo à norma SER 19794-2) e receber o resultado da avaliação das métricas de performance. Mais detalhes podem ser encontrados no site oficial do FVC¹⁹.

Abaixo se encontra tabela com valores de FAR e FRR para testes realizados em 2003, 2006 e 2008.

Evaluation	Data	Best reported accuracy
NIST FpVTE 2003 (MST)	10,000 plain fingerprints	FNMR = 0.6% at FMR = 0.1%
FVC2006	140 fingers × 12 images Electric field sensor (250 ppi) Optical sensor (569 ppi) Sweep sensor (500 ppi)	FNMR = 15% at FMR = 0.1% FNMR = 0.02% at FMR = 0.1% FNMR = 3% at FMR = 0.1%
NIST ELFT 2008 (Phase II)	835 latent prints, 100,000 rolled fingerprints	FNIR = 8% at FPIR = 1%

Figura 10 – Valores FAR (FNMR) e FMR (FRR) para impressão digital

¹⁹ [www. http://bias.csr.unibo.it/](http://bias.csr.unibo.it/)

(Fonte: Fingerprint Matching – NANDAKUMAR, Karthik et al. Anil K. Jain, Michigan State University Jianjiang Feng, Tsinghua University, Beijing. 2010.)

Observações: Na tabela supracitada, a linha 1 refere-se aos resultados de FNMR e FMR do FpVTE 2003, a linha 2 aos mesmos indicadores para a FVC 2006 (separados por sensores) e a linha 3 está relacionada aos resultados da aplicação para fragmentos de impressão digital.

Considerando-se o programa indiano (UIDAI), para 84 milhões de pessoas, o FTC (equivalente próximo ao FTA) foi de 0,14%, (para impressão digital e íris simultaneamente) com um FAR de 0,035% para o processo de identificação.

Para o processo de verificação, com um FAR de 0,01%, o FRR para a impressão digital foi de 0,71% (enquanto que para a íris o FRR foi de 0,22%) (Gelb e Clark, 2013).

5.2.6 Aceitabilidade

A impressão digital está associada à história da identificação civil no país, sendo, portanto, um ponto positivo.

Por outro lado, aspectos como o contato físico entre a pele do cidadão e o leitor biométrico, juntamente com a associação ao uso da impressão digital para fins criminais, são vistos por muitos como um fator negativo.

Diante do exposto, a aceitabilidade da impressão digital pode ser considerada mediana, fato que também pode ser comprovado em tabelas conhecidas que tratam destas avaliações. (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006)

5.2.7 Resistência à fraude

Normalmente é utilizado um dedo falso de silicone ou algum outro tipo de plástico para reproduzir a digital. Casos em que há a amputação e subsequente utilização do referido dedo não se mostram tão eficazes, funcionando apenas em alguns poucos leitores (normalmente mais antigos, sem identificação de vivacidade) (Geradts e Sommer, 2006).

Estima-se que o uso de sensores e algoritmos para detecção de vivacidade reduzam o percentual de detecção incorreta ou fraude, de 90% para 10%. (FpVTE, 2003)

Ressalta-se que, em sistemas que utilizam coleta de vários dedos através de sensor monodactilar (para apenas um dedo), há vulnerabilidade em relação à sequência de

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.62/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

registro das impressões digitais coletadas caso a ordem dos dedos seja alterada.

De acordo com as bibliografias consultadas, a característica é avaliada como mediana (Klokova, 2010) e (Jain et al, 2004).

5.3 ESTIMATIVA DE CUSTO

Considerando uma meta física de 10,8 milhões de eleitores, o TSE estimou que o custo do recadastramento seria de R\$ 4,00²⁰ por eleitor, conforme especificado abaixo.

“Nos termos da justificação da Resolução: “A SOF informou existir no Projeto de Lei Orçamentária Anual – PLOA 2011, para o presente exercício, dotação de R\$ 51.000.000,00 para as ações envolvendo a biometria, dos quais R\$ 43.475.324,00 destinados ao custeio administrativo e R\$ 7.524.676,00 a investimento. Acrescentou que “a meta física constante do PLOA 2011 para o referido projeto é cadastrar 8% do eleitorado nacional, representando 10,8 milhões de eleitores, o que possibilitaria um dispêndio médio da ordem de R\$ 4,00 por eleitor”.

Em relação ao processo de cadastramento para identificação civil na Índia (UIDAI), o valor total do processo unitário por usuário cadastrado é de aproximadamente U\$2,15 (130 IND²¹).

Estimativas de preços de equipamentos em licitações recentes (2 milhões de pessoas) no Brasil podem ser visualizadas a seguir:

Tabela 8 – Estimativa do custo da impressão digital.

Fabricante	Descrição	Valor unitário (R\$)	Valor (R\$)
01	Latentes (equipam., dispositivos, acessórios e software)	6,49	1.366.050,00
	AFIS (equipam., dispositivos, acessórios e software)		11.610.500,00
	TOTAL		12.976.550,00

²⁰ Marcos Köhler – Vale a pena fazer o recadastramento biométrico eleitoral? – www.brasil-economia-governo.org.br

²¹ <http://www.moneylife.in/article/nandan-nilekani-learning-kannada-for-elections/35583.html>

02	Latentes (equipam., dispositivos, acessórios e <i>software</i> .)		3.177.218,61
	AFIS (equipam., dispositivos, acessórios e <i>software</i>)	5,98	8.776.054,86
	TOTAL		11.953.273,47

5.4 CARACTERÍSTICAS DA COLETA

5.4.1 Idade inicial

A formação das impressões digitais acontece nos primeiros sete meses de gestação e permanecem intactas por toda a vida, embora a União Européia recomende a coleta somente a partir dos 6 anos de idade, segundo (Guenter, 2013). Para crianças, os tamanhos das estruturas das impressões digitais mais relevantes (em particular, a distância entre os sulcos) são até um terço menores do que para os adultos.

5.4.2 Tamanho do arquivo gerado

O tamanho do arquivo gerado na coleta da impressão digital varia de acordo com a resolução e o tamanho da imagem. (Costa, 2001) apresenta um comparativo mostrando que diferentes sensores, trabalhando com uma mesma resolução, podem gerar arquivos de diferentes tamanhos.

Segundo especificações de alguns fabricantes de sistemas de coleta eletrônica da impressão digital, o tamanho das imagens geradas varia entre 256, 384 e 512 bytes.

Outro fabricante informa que o tamanho do *template* pode variar de 200 a 5000 bytes²².

5.4.3 Tempo de coleta

²² http://www.griaulebiometrics.com/pt-br/faq_biometrics

O tempo gasto com o cadastramento da impressão digital de adultos (três imagens – 4/4/2 – batido) é de aproximadamente 2 minutos (1m51s) e para crianças o tempo é menor, de aproximadamente 1,5 minutos (1m13s) (UIDAI 2012b).

O tempo de coleta para o passaporte brasileiro é em torno de 1 a 2 minutos.

Segundo informações do site do SER-RN²³, a expectativa é que sejam atendidos, diariamente, 4 mil eleitores, com uma média de tempo de atendimento de 20 minutos. O tempo informado está relacionado ao cadastramento completo, inclusive com o registro de foto da face do cidadão.

5.5 ALGORITMOS DE RECONHECIMENTO

A avaliação de quão bom um algoritmo é para realizar a identificação de uma determinada biometria depende de qual característica se está analisando: EER, FRR, FAR, velocidade de comparação, velocidade de cadastramento, tamanho do banco de dados, dentre outras.

Além disso, ano após ano, são realizadas competições para se verificar quais algoritmos apresentam melhores resultados. Conforme supracitado, tem-se o FVC – *Fingerprint Verification Competiton* e a FpVTE – *Fingerprinte Vendor Technology Evaluation* (NIST).

5.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Em virtude de significativa parte (14,2%) (Censo IBGE, 2010) da população brasileira desempenhar funções nas atividades da agricultura, pecuária, produção florestal, pesca e aquicultura, e outros em atividades vinculadas ao serviço doméstico (6,9%) (Censo IBGE, 2010), há a possibilidade de que parte destas pessoas tenha suas digitais gastas ou inexistentes.

Considerando-se a população brasileira com 200 milhões de pessoas, defere-se que 42,2 milhões de pessoas são potencialmente passivas de danos ou desgastes nas digitais e poderão estar excluídas do processo de identificação biométrica (quando utilizando apenas esta biometria).

²³ <http://www.tre-rn.jus.br/noticias-tre-rn/2013/Julho/recadastramento-biometrico-de-natal-comeca-dia-17>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.65/125
--------------------	---------------------	---	------------

Confidencial.

5.7 UTILIZAÇÃO EM OUTROS PAÍSES

Em geral, a maioria dos países já utilizam a impressão digital como padrão para identificação civil: Argentina, Bolívia, Chile, Colômbia, Equador, Guatemala, México, Peru, Alemanha, Bélgica, Espanha, República Tcheca, Portugal, Gambia, Nigéria, Índia, Indonésia.

Destes, Índia, Indonésia e México já utilizaram a impressão digital como uma de suas biometrias para identificação em sistemas de grande escala.

Fabricantes internacionais: NEC, L1, SAGEM/MORPHO, ANTHEUS, DERMALOG (MONTREAL), COGENT (3M), SUPREMA, DIGITAL PERSONA, ANVIZ, AWARE, ZKTECO, GREEN BIT, SMARTMATIC, BIO-KEY, SAFRAN).

No Brasil, tem-se a empresa GRIAULE²⁴ (Campinas/SP), vencedora da licitação para fornecimento de solução de identificação para o TSE (Tribunal Superior Eleitoral), a qual fornece soluções como plataforma e equipamentos para identificação através de impressão digital.

Foram encontradas algumas empresas nacionais cujos produtos estão relacionados à área de identificação, controle de acesso e segurança, baseados na biometria impressão digital, dentre elas a AKIYAMA²⁵ (Curitiba/PR) parceira da Sarnoff, VERIDIS²⁶ (Campinas/SP), FINGERTECH²⁷ (Londrina/PR), TECHMAG²⁸ (São Paulo/SP), porém sem soluções dedicadas à identificação em larga escala.

5.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

No caso da impressão digital, essa biometria é muito bem utilizada tanto para identificação como para verificação.

Em relação ao programa indiano (UIDAI 2012c), para 84 milhões de pessoas, o FTC (equivalente próximo ao FTA) foi de 0,14%, (para impressão digital e íris utilizados simultaneamente) juntamente com um FAR de 0,035% quando considerado o processo

²⁴ Griaule - <http://www.griaulebiometrics.com/>

²⁵ Akiyama - http://akiyama.com.br/site/index.php?option=com_contentview=articleid=61eItemid=208

²⁶ Veridis Biometrics - <http://www.veridisbiometrics.com/>

²⁷ Fingertech - <http://nitgen.com.br/>

²⁸ TechMag - <http://techmag.com.br/>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.66/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

de identificação.

Segundo (Gelb e Clark, 2013), considerando-se o processo de verificação, para um FAR de 0,01%, o FRR para a impressão digital foi de 0,71% (enquanto que para a íris o FRR foi de 0,22%).

5.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

Diante do legado existente no cadastramento eleitoral e criminal no país e considerando as características já apresentadas, a impressão digital é uma biometria fortemente aplicável à individualização do brasileiro.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.67/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

6 ÍRIS

6.1 INTRODUÇÃO

Segundo (Ross et al, 2006), a íris é a região anular de cada um dos olhos e é delimitada pela pupila e pela esclera (o branco do olho). A textura visual da íris é formada durante o desenvolvimento fetal e se estabiliza durante os dois primeiros anos de vida. De acordo com (Ross et al, 2006), a pigmentação, no entanto, continua mudando ao longo de um período prolongado de tempo.

A complexa textura da íris carrega muita informação distinta útil para o reconhecimento pessoal (Daugman, 2004). A precisão e velocidade dos sistemas de reconhecimento atualmente desenvolvidos baseados em íris são promissoras e apoiam a viabilidade de sistemas de identificação em larga escala.

Cada íris é diferente e até mesmo as íris de gêmeos idênticos são diferentes.

De acordo com (Daugman, 1999), é possível detectar lentes de contato impressas com uma íris falsa.

O movimento do olho pode também ser usado como uma medida de vivacidade para esta biometria.

Segundo (Jain et al, 2004), os primeiros sistemas de reconhecimento por íris requeriam considerável participação do usuário e eram caros, já os novos sistemas tornaram-se mais amigáveis e de baixo custo.

Etapas do Processo

O sistema de reconhecimento da íris pode ser descrito em quatro etapas. Em primeiro lugar, uma imagem contendo o olho do usuário é capturada pelo sistema. Em seguida, a imagem é pré-processada para normalizar a escala de tamanho, a iluminação e localizar a íris. Em terceiro lugar, são apresentados os padrões extraídos e finalmente, a decisão é feita por meio de correspondência ou não da imagem colhida com a armazenada.

(Zhu et al, 2000) descrevem as etapas a seguir.

Aquisição da imagem da íris

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.68/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

O primeiro passo para o reconhecimento da íris é a sua coleta. A íris é pequena e muitas vezes escura, tornando difícil a aquisição de boas imagens para análise, principalmente se a câmera utilizada for comum. Por isso existem equipamentos específicos para a aquisição da imagem da íris e eles são projetados para que a coleta seja feita com a qualidade necessária.

Pré processamento (segmentação e normalização)

A imagem que é coletada contém não apenas a parte útil, ou seja, a íris, como também partes que serão irrelevantes para a comparação, como, por exemplo, parte da pálpebra e a parte branca do globo ocular. O sistema então faz o recorte da imagem da íris e a equaliza a luz que incidiu sobre a imagem no momento da coleta compensando a questão do brilho dos olhos que varia de acordo com sua lubrificação. Além disso, se a coleta é feita a partir de diferentes distâncias entre o olho e a câmera, haverá a geração de imagens com diferentes tamanhos, exigindo também uma adequação. Essa adequação também é feita neste momento. Ou seja, para efeitos de análise, a imagem precisa ser processada, o que ocorre em três etapas, conforme a seguir:

1º. Localização da íris. Tanto o limite interno quanto o limite externo de uma íris são circulares, mas geralmente estes dois círculos não são concêntricos. Em comparação com o restante do olho, a pupila é muito mais escura, facilitando a detecção dos limites por meio de uma limiarização de cores. O limite interno se mede comparando a cor da pupila com a cor da íris e o externo, fazendo-se a comparação da cor da íris com a cor branca do globo ocular.

2º. Adequação da íris. O tamanho da pupila pode mudar devido à variação da iluminação. Esta variação, associada às deformações elásticas na textura da íris, pode interferir com os resultados de correspondência de padrão. Para que a análise da textura seja precisa é necessário compensar esta deformação e uma vez que os limites da íris forem detectados, pode-se mapear o seu anel para um bloco retangular de textura e tamanho fixos.

3º. Aperfeiçoamento da imagem. A imagem original da íris tem baixo contraste e a iluminação pode não ser uniforme em virtude da posição da fonte de luz utilizada na coleta. Estes fatores podem prejudicar o resultado da análise da textura. Desta forma faz-

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.69/125
--------------------	---------------------	---	-------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

se necessário o melhoramento da imagem da íris, equalizando-a por meio da redução do efeito da iluminação. Após a equalização, utiliza-se somente a parte interna da imagem da íris em virtude da oclusão causada pelas pálpebras. A Figura 11 mostra o resultado do pré-processamento da imagem da íris.

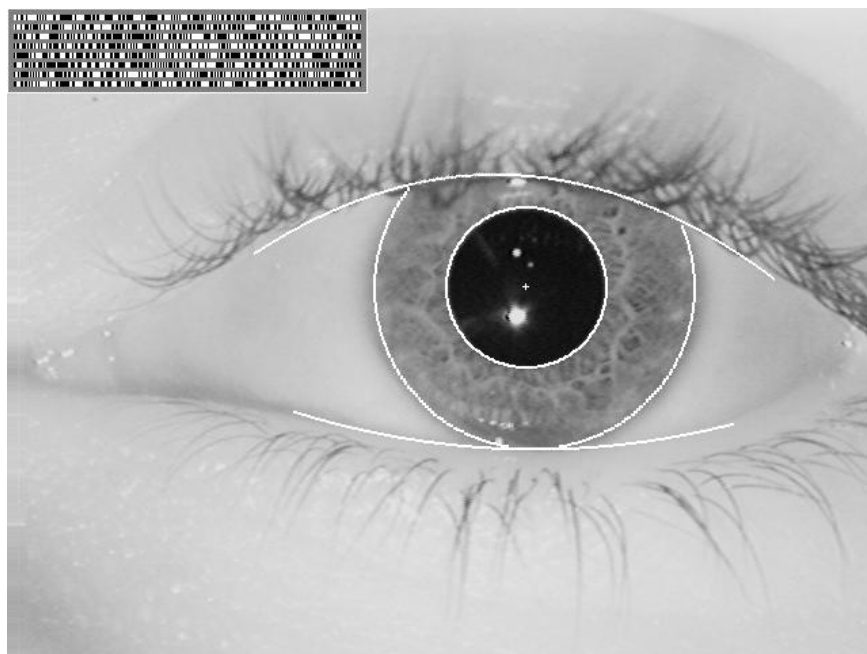


Figura 11 – Resultado do pré-processamento da imagem da íris.

Fonte: (Costa et al, 2006)

Segundo (Carreira, 2009), os métodos de segmentação da íris mais relevantes são:

- Método de John Daugman;
- Método de Richard P. Wildes;
- Método de Ma et al.;
- Método de Zhaofeng He et al.

Extração de características da íris

(Zhu et al, 2000) utilizaram dois métodos de análise de texturas para extrair características do bloco normalizado de textura de imagem. Tais métodos são conhecidos como Filtro de Gabor e Transformada 2-D de Wavelet.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.70/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

De acordo com (Carreira, 2009), os métodos de extração de características mais conhecidos são:

- Método de John Daugman;
- Método de Richard P. Wildes;
- Método de Ma et al.

Segundo (Carreira, 2009), é na extração de características que se faz uso das propriedades da íris para criar uma assinatura biométrica.

Filtragem multicanais de Gabor.

Segundo (Zhu et al, 2000), a filtragens multicanais de Gabor é inspirada nos resultados de estudos psicofísicos que mostram o tratamento da informação de imagem no córtex visual humano e que envolve um conjunto de mecanismos paralelos e quase independentes ou canais corticais que podem ser modelados por pares de filtros. Resumidamente, cada canal cortical é composto por um par de filtros Gabor $h_e(x, y, f, \theta)$ e $h_o(x, y, f, \theta)$. Estes filtros são simétricos e dados pela equação:

- $h_e(x, y) = g(x, y) \cdot \cos[2\pi f(x \cos\theta + y \sin\theta)]$
- $h_o(x, y) = g(x, y) \cdot \sin[2\pi f(x \cos\theta + y \sin\theta)]$

em que $g(x, y)$ é uma função “2-D gaussian”, f e θ são, respectivamente, a frequência central e orientação, que definem a localização do canal no plano das frequências. Para cada frequência escolhida (em geral são utilizadas potências de 2), geram-se imagens filtradas para alguns valores de θ , a partir das quais são extraídas as características.

Transformada 2-D de Wavelet.

De acordo com (Zhu et al, 2000), a Transformada 2-D de *Wavelet* é uma boa ferramenta de análise e tem sido usada para o reconhecimento da textura da íris. Essa transformada 2-D pode ser tratada como duas transformadas *wavelet* separadas. Depois de aplicar transformação *wavelet* em uma imagem original, um conjunto de sub-imagens é

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.71/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

obtido em diferentes níveis de resolução. A média e a variância de cada sub-imagem *wavelet* são extraídas como características de textura. As informações no nível de resolução mais fina podem ser fortemente afetadas por ruídos produzidos pela equação. A fim de reduzir este efeito sobre as características extraídas, apenas cinco níveis de baixa resolução são utilizados e se exclui o nível mais grosseiro. Para cada nível de resolução, médias e desvios padrão são extraídos como recursos. Isso faz com que as 26 características extraídas sejam robustas mesmo em um ambiente ruidoso.

Identificação da Íris.

O reconhecimento da íris, baseado em vetores de características, trata-se de um problema de reconhecimento de padrões. Em princípio, pode-se usar qualquer tipo de classificador.

6.2 CARACTERÍSTICAS TÉCNICAS

6.2.1 Universalidade

De acordo com (Gelb e Clark, 2013), a primeira conclusão é que a autenticação pela íris é mais abrangente do que a autenticação via impressões digitais. Suas taxas FTC (*Failure to Capture*) foram muito menores: apenas 0,33 por cento da amostra não foi capaz de fornecer leituras suficientemente boas da íris, em comparação com cerca de 1,7 por cento para impressões digitais, mesmo tendo a opção de escolher os dois melhores dedos.

De acordo com (Olatinwo et al, 2013), a aniridia (ausência de íris) ocorre em 1,8 a cada 100.000 (cem mil) nascimentos.

Considerando a população de 200 milhões de habitantes, ter-se-ia, potencialmente, 3.600 pessoas com ausência de íris no Brasil.

De acordo com (Jain et al, 2004) e (Moraes, 2006), a biometria recebe nota máxima em relação a esta característica. (Moraes, 2006) atribui nota 5 à mesma.

6.2.2 Singularidade

De acordo com (Mali e Bhattacharya, 2013), a íris tem uma textura fina que, como as

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.72/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

impressões digitais, é determinada aleatoriamente durante a gestação embrionária. Mesmo os indivíduos geneticamente idênticos têm texturas de íris completamente diferentes, ao passo que o DNA não é exclusivo para cerca de 0,2% da população humana que têm um irmão gêmeo geneticamente idêntico.

A singularidade dessa biometria é valorada como excelente, recebendo notas máximas (5) de acordo com vários autores (Jain et al, 2004) e (Moraes, 2006).

6.2.3 Permanência

De acordo com (Mali e Bhattacharya, 2013), embora existam alguns procedimentos cirúrgicos que possam afetar a cor e a forma geral da íris, a textura fina permanece bastante estável ao longo de muitas décadas. Há relatos de comparações de íris feitas com sucesso pelo período de 30 anos.

Desta forma, é dada nota máxima a esta característica biométrica (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

6.2.4 Coletabilidade

De acordo com (Mali e Bhattacharya, 2013), uma varredura da íris é semelhante a se tirar uma fotografia e pode ser realizada a partir de cerca de 10 cm até poucos metros de distância (aproximadamente três metros). Para a coleta da biometria, não há a necessidade do contato com qualquer equipamento, eliminando assim qualquer rejeição ao procedimento de coleta devido à deposição de resíduos deixados anteriormente, como no caso do escaneamento de retina, no qual existe a necessidade de se posicionar o olho muito próximo a uma lente (como olhar para uma lente de microscópio).

A coleta desta biometria pode ser realizada de forma monocular ou binocular e é extremamente rápida e precisa, tornando o sistema de identificação mais seguro.

O usuário precisa simplesmente posicionar-se em frente a uma câmera, por meio da qual uma quantidade muito fraca de iluminação infravermelha é usada, fazendo com que o sistema seja perfeitamente seguro em relação à sua integridade física.

Esta característica é avaliada como mediana – nota 3 (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006). Essa avaliação pode ser justificada em função da íris ser um alvo de tamanho pequeno e que está em constante movimento. A íris também é localizada atrás de uma superfície curvada, úmida e refletiva. Ela pode ser obscurecida por cílios,

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.73/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

lentes, óculos e pelas pálpebras. Em função das propriedades do olho, a iluminação pela luz influencia a forma e a presença total da íris (Champod et al, 2005).

6.2.5 Desempenho

O desempenho de uma biometria está relacionado a parâmetros como velocidade de cadastramento, velocidade de comparação, tempo de coleta, FAR, FRR, EER, FTA, etc.

Os parâmetros mais comuns a serem utilizados para se verificar o desempenho de um sistema biométrico para identificação são o FAR e FRR.

A seguir são apresentadas duas tabelas com valores comparativos de FRR para casos estipulados de FAR utilizando a íris sozinha ou em conjunto com impressão digital, com base nas experiências obtidas do programa de identificação da Índia.

1. Authentication: Detection Error Tradeoff (DET) of Iris and Fingerprints

False Rejection Rate (FRR)	False Acceptance Rate (FAR)			
	1.0E-06	1.0E-05	1.0E-04	1.0E-03
2 irises, dual camera	0.27%	0.23%	0.22%	0.21%
2 irises, single camera	0.46%	0.34%	0.33%	0.31%
2 fingers, labeled			0.70%	0.42%
2 fingers, unlabeled			1.09%	0.74%
1 finger, labeled			2.47%	1.37%
1 finger, unlabeled			3.41%	2.04%
2 irises, dual camera x 2 fingers, labeled			0.0015%	0.0009%

2. Authentication: Detection Error Tradeoff (DET) of Iris and Fingerprints

False Rejection Rate (FRR)	False Acceptance Rate (FAR)					FTC
	1.0E-06	1.0E-05	1.0E-04	1.0E-03		
2 irises, dual camera	0.60%	0.56%	0.55%	0.54%	Iris	0.33%
2 irises, single camera	0.79%	0.67%	0.66%	0.64%	Finger	1.68%
2 fingers, labeled			2.38%	2.10%		
2 Fingers, unlabeled			2.77%	2.42%		
1 finger, labeled			4.15%	3.05%		
1 finger, unlabeled			5.09%	4.73%		
2 irises, dual camera x 2 fingers, labeled			0.0131%	0.0113%		

Figura 12 – Taxas de FAR e FRR para a biometria da íris.

Fonte: (Gelb e Clark, 2013).

A característica desempenho é avaliada como alta – nota 5 (Klokova, 2010), (Jain et al, 2004) e (Moraes, 2006).

De acordo com (Modi, 2011), o algoritmo de reconhecimento proposto por Daugman realiza o cálculo de uma métrica denominada *Hamming Distance* (HD) para a comparação de dois códigos de íris (*IrisCodes*).

Para cada correspondência de bit nos dois códigos de íris que estão sendo analisados, a qualidade dos correspondentes bits de máscara é verificada. Se ambos os bits de máscaras indicam que os bits do *IrisCode* são usáveis, eles são comparados. Este processo é realizado em todo o código *IrisCode* e o número de bits que estão em divergência é calculado.

A nota final é calculada da fração entre os bits que estão em divergência, depois que os bits inutilizáveis tenham sido descartados. Esta nota é comparada ao *threshold* (limiar) do sistema que resulta em uma decisão. Na maioria dos sistemas que utilizam o algoritmo de reconhecimento de Daugman, este limiar gira em torno de 0,32, de acordo com a Figura 13.

O algoritmo de reconhecimento de Daugman apresenta vários benefícios, sendo o principal a velocidade (extremamente rápido) de comparação, já que se trata de uma comparação bit-a-bit (*bitwise*).

HD Criterion	Odds of False Accept	Odds of False Reject
0.25	1 in 13.5 billion	1 in 1,490
0.26	1 in 2.04 billion	1 in 2,660
0.27	1 in 339 million	1 in 4,850
0.28	1 in 60 million	1 in 9,000
0.29	1 in 12 million	1 in 17,100
0.30	1 in 2.4 million	1 in 32,800
0.31	1 in 603,000	1 in 64,200
0.32	1 in 151,000	1 in 128,000
0.33	1 in 39,800	1 in 260,000
0.34	1 in 11,500	1 in 536,000
0.35	1 in 3,630	1 in 1.12 million

Figura 13 – Probabilidades individuais de Falsa Aceitação e Falsa Rejeição

Fonte: (Daugman, 1994)

6.2.6 Aceitabilidade

Em virtude do desenvolvimento, evolução e amadurecimento da tecnologia de reconhecimento da íris, desmistificou-se o conceito relacionado aos efeitos colaterais gerados pelo feixe de luz utilizado para a coleta da imagem da íris. Trata-se de uma visão equivocada sobre a técnica por falta de popularização e conhecimento da tecnologia, inclusive porque atualmente utiliza-se feixe de infravermelho.

Referências bibliográficas anteriores ao fim da vigência da patente, popularização da tecnologia e adoção do uso da íris em programas de identificação de grande escala (Índia, Indonésia e México), mostram que a característica é avaliada como baixa (Jain et al, 2004) e (Moraes, 2006).

Contudo, considerando que a Aceitabilidade está relacionada ao conforto e aceite do uso da tecnologia pelo usuário, em literatura mais recente, relacionada à característica Conforto, esta biometria foi avaliada como alta – nota 8 em 9 (Carreira, 2009).

Tendo como base o recente estudo realizado para implementação de sistema de identificação na Índia (UIDAI 2012c), a característica Conforto foi considerada como um dos principais benefícios da adoção da tecnologia de íris para individualização. Isso se deve ao fato da coleta não ser intrusiva, já que não há contato físico com usuário, tornando-se uma experiência cômoda. A experiência é similar a se tirar uma fotografia do indivíduo, exceto pelo fato da câmera estar mais próxima da face durante a captura da imagem.

Diante do exposto, a característica é considerada mediana.

6.2.7 Resistência à fraude

As fraudes mais comuns ocorrem no momento da identificação. Uma pessoa pode perfeitamente utilizar uma foto de um olho para passar pelo reconhecimento de íris. Para evitar esse tipo de fraude, os equipamentos de reconhecimento de íris mais atuais possuem uma luz infravermelha para iluminar o olho do indivíduo e detectar a pupila em movimento. Comumente, podem ser realizados dois tipos de verificação por meio de um *software* que analisa (baseado em algoritmos programados) as características usadas para diferenciar a íris na imagem fornecida pelo sensor e por meio de uma abordagem que utiliza o *hardware*, principalmente observando a oscilação permanente da pupila quando exposta à iluminação. Outras técnicas de fraude são a utilização de lentes de contato personalizadas (Geradts e Sommer, 2006) e a remoção do olho da pessoa (Murari, 2013). Essa última não é eficaz, já que após retirado, o olho se deteriora rapidamente.

Um questionamento muito comum é se a utilização de lentes de contatos pode influenciar ou não o sistema de identificação pela íris. Quando a lente de contato utilizada for a gelatinosa, o sistema de reconhecimento não é afetado já que esta não altera em nada a imagem da íris (possibilita a identificação das bordas da pupila e da íris, além de não alterar em nada os cílios e as sobrancelhas). Porém, quando se trata de lentes de contato “*patterned*”, que são lentes de contato customizadas, estas cobrem o tecido da íris, impossibilitando o reconhecimento da mesma. Caso seja utilizado esse tipo de lente,

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.77/125
--------------------	---------------------	---	------------

Confidencial.

o sistema deverá reconhecer a lente fora do padrão e negar qualquer acesso (Murari, 2013).

Esta característica é considerada alta, nota 5, o que significa que a íris é pouco susceptível a fraude (Klokoova, 2010), (Jain et al, 2004) e (Moraes, 2006).

6.3 ESTIMATIVA DE CUSTO

De acordo com informações em (UIDAI 2012d), estima-se que o custo da inclusão da íris como biometria do projeto indiano é de 4,4 IND (US\$ 0,07) por pessoa, para a população indiana (aproximadamente 1,2 bilhões de pessoas).

Este custo está dividido em três categorias, a saber.

Tabela 9 – Custo da íris do projeto indiano.

Componente	Custo por cadastramento
Dispositivo de captura (sensor)	2,9 IND (US\$ 0,048)
Procedimento de captura	0,75 IND (US\$ 0,012)
Custo <i>software</i> de-duplicação	0,75 IND (US\$ 0,012)

A estimativa do custo se baseia nas seguintes premissas.

- O preço do sensor de captura da íris permanecerá em 100.000 IND (US\$ 1.662,00);
- A câmera da íris tem vida útil de no mínimo três anos;
- O tempo de captura da íris é de aproximadamente um minuto;
- O preço do *software* de reconhecimento da íris não será alterado com o passar do tempo.

Estimativas de preços de equipamentos em licitações recentes (considerando 2 milhões de pessoas) podem ser visualizadas a seguir.

Tabela 10 – Estimativa do custo da íris.

Fabricante	Descrição	Valor Unitário (R\$)	Valor (R\$)
01	Equipamentos, dispositivos, acessórios e <i>software</i>	1,27	2.550.00,00
02	Equipamentos, dispositivos, acessórios e <i>software</i>	1,16	2.323.456,47

6.4 CARACTERÍSTICAS DA COLETA

6.4.1 Idade inicial

Segundo (Muroò et al, 2000), a íris começa a ser formada a partir do terceiro mês de gestação e a estrutura completada aos oito meses de gestação. No entanto a pigmentação continua a ser formada até o primeiro ano de vida.

A sua cor é dada através do tipo e da quantidade de pigmentos no tecido da íris, sendo a azul a cor com menos pigmentação.

A idade mínima recomendada para coleta é de 4 anos (México) e de 5 anos (Índia).

6.4.2 Tamanho do arquivo gerado

Segundo o site IRIS ID²⁹, um *template* da íris não cifrado tem tamanho de 512 bytes.

De acordo com (Modi, 2011), o *template* de 256 bytes também é chamado de *IrisCode*.

6.4.3 Tempo de coleta

²⁹ <http://www.irisid.com/>

Segundo informações de implementação do programa de identificação indiano (UIDAI 2012c), o tempo para coleta é de aproximadamente 52 segundos.

6.5 ALGORITMOS DE RECONHECIMENTO

A avaliação de quão bom um algoritmo é para realizar a identificação de uma determinada biometria depende de qual característica se está analisando: EER, FRR, FAR, velocidade de comparação, velocidade de cadastramento, tamanho do banco de dados, dentre outras.

Além disso, ano após ano, são realizadas competições para se verificar quais algoritmos apresentam melhores resultados, como é o caso da *Iris Exchange* (NIST).

O NIST também iniciou o projeto IREX-II com o objetivo específico de definir e medir a qualidade das imagens de íris, indicando a sua importância para a comunidade de padronização, principalmente para aplicações de larga escala (Modi, 2011).

6.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Como já informado anteriormente, a universalidade desta biometria é elevada, inclusive na população brasileira. Acredita-se que não haja influências restritivas do trabalho ou da cultura do brasileiro em relação à utilização da íris como biometria para identificação.

6.7 UTILIZAÇÃO EM OUTROS PAÍSES

Os países que já utilizam essa biometria são: Índia, Indonésia e México.

Dentre os principais fabricantes internacionais, encontram-se: SUPREMA, NEC, PRECISION, INFORMATIC, SAGEM/MORPHO, SMART IDENTITY, BIO ENABLE TECHNOLOGY, INSPIRA BIOMETRICS, IRIS ID (LG), ANVIZ, SRI SARNOFF, SMARTMATIC, CROSS MATCH TECHNOLOGIES³⁰.

No Brasil existem algumas empresas como a ANTHEUS³¹ (Curitiba/PR), que possui soluções utilizando a íris para identificação de indivíduos em residências e outras

³⁰ STQC Directorate - Department of Information Technology, New Delhi e www.findbiometrics.com

³¹ Antheus - <http://www.antheus.com.br/produtos>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.80/125
--------------------	---------------------	---	------------

Confidencial.

aplicações menores.

6.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

Segundo (Delgado, 2013), atualmente, a íris é considerada a biometria mais precisa. Desta forma, é extremamente indicada para identificação em sistemas de grande escala.

De acordo com o projeto desenvolvido pela Índia, a íris tem sido utilizada principalmente na identificação para de-duplicação dos usuários, evitando-se inserções em duplicata e mantendo-se um enorme banco de dados limpo.

Assim como para a identificação, essa biometria também pode ser muito bem utilizada para verificação (1:1).

6.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

Verifica-se que a íris possui excelentes características como precisão, velocidade de cadastramento, singularidade e universalidade.

O reconhecimento da íris é uma tecnologia recente, considerando outras já sedimentadas. Entretanto, tem despertado bastante atenção de fabricantes e de vários governos em todo o mundo. Os principais benefícios em se utilizar a íris são o aumento da precisão no reconhecimento de indivíduos e o fato da inclusão, nos programas de identificação, de pessoas que não possuem impressões digitais, aumentando a população coberta pelo sistema.

O uso da íris é aplicável ao projeto RIC devido às vantagens anteriormente mencionadas e pelo fato do sistema RIC ser considerado um projeto de grande escala.

7 VEIAS DA MÃO

7.1 INTRODUÇÃO

O padrão formado pelos vasos sanguíneos é único para cada indivíduo. O reconhecimento pelas veias das mãos é feito utilizando luz infravermelha que identifica as hemoglobinas do sangue com oxigênio, separando-as por cores (as veias aparecem em cores escuras). A rede de vasos da mão é muito complexa, permitindo, portanto, que os padrões das veias sejam considerados únicos para cada indivíduo.³²

As veias e artérias, assim como os capilares, constituem os vasos sanguíneos do sistema circulatório do nosso corpo. As artérias correspondem àqueles vasos que saem do coração e por isso estão sob alta pressão constantemente. Portanto, as paredes dos vasos arteriais requerem maior elasticidade e espessura para manter adequada a oxigenação das células. As veias são os vasos que chegam ao coração com grandes volumes de sangue.

A possibilidade de usar o padrão vascular da mão data de meados de 1990, tendo o primeiro produto comercial neste sistema desenvolvido em 1997, o BK-100, pela BK Systems (Jain et al, 2007). Desde então, a tecnologia tem se desenvolvido, e foi adotado em 2007 pela Organização Internacional de Padronização (*International Standard Organization*, ISO) (Petitimbert et al, 2011).

Segundo (Nadort, 2007), os destaques na indústria de leitura de padrões vascular da mão podem se destacar por região da mesma. A Luminetx, Techsphere e Nextern têm tecnologias voltadas para o dorso da mão. Quanto à palma, a Fujitsu é líder com seu dispositivo *PalmSecure*. Na captura de veias do dedo, destacam-se a PosID, e principalmente a Hitachi, com várias patentes. Para fins de informação, a biometria das veias do pulso é rara e sem marco comercial, com destaque somente para a patente de Joseph Rice de 1997, de identificação de indivíduos. (Wilson, 2011) nota que as cinco desenvolvedoras chave em reconhecimento do padrão de veias são asiáticas: Bionics, Fujitsu, Hitachi, Sony e Techsphere. A MorphoTrak é listada pelo site findBiometrics³³ como vendedora de produtos reconhecimento vascular.

A característica mais relevante desta biometria é a sua resistência à fraude, já que o

³² <http://www.lcg.ufrj.br/Members/rafael/Biometria>

³³ <http://findbiometrics.com/solutions/vein-recognition/>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.82/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

padrão das veias da mão é interno ao corpo, tornando-o difícil de ser copiado.

José Alberto Canedo descreve que as informações existentes sobre a biometria foram originadas, principalmente, pela própria Fujitsu (empresa detentora da patente da biometria) usando uma base privada. Adicionalmente, afirma que existe pouca pesquisa em desenvolvimento sobre veias, não havendo muita referência sobre o assunto no meio acadêmico. Além disso, salienta a inexistência de uma competição pública voltada para a biometria das veias que mostre o estado da arte desses algoritmos, não existindo ainda resultados gerados por organismos independentes, a exemplo da impressão digital, íris e face³⁴.

ETAPAS DO PROCESSO

Segundo (Wang e Leedham, 2005), um sistema biométrico de reconhecimento do padrão das veias pode ser caracterizado por 5 fases: aquisição da imagem da mão, tratamento da imagem, segmentação dos padrões de veias, “*Skeletonization*” (que seria o registro dos padrões segmentados, porém em linhas finas, ou seja, o esqueleto do padrão das veias) e comparação, as quais são explicadas a seguir.

- Aquisição da Imagem da Mão

As veias ficam escondidas sob a pele, porém as mais superficiais possuem temperatura mais alta que os tecidos ao seu redor. Em virtude deste fato, o padrão das veias pode ser coletado por uma câmera térmica, como pode ser visualizado na Figura 14 capturada em ambiente com temperatura entre 20° a 25° C.

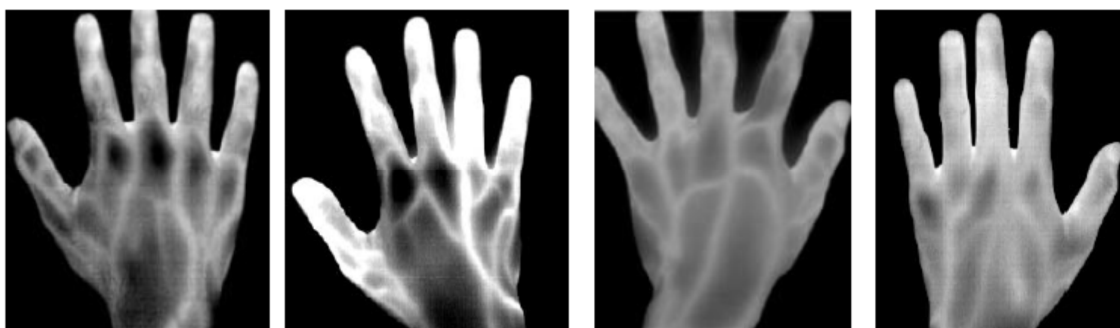


Figura 14 – Aquisição de imagem das veias da mão por meio de câmera térmica em ambiente com temperatura de 20° a 25° C

³⁴ <http://www.forumbiometria.com/artigos/36-geral/48-biometria-das-veias-da-mao-hand-veins.html>

Fonte: (WANG e LEEDHAM, 2005).

A qualidade da imagem adquirida pode ser influenciada por condições ambientais, principalmente a temperatura e umidade. Isso fica evidente na Figura 15, tirada em ambiente cuja temperatura variava de 30° a 35°.

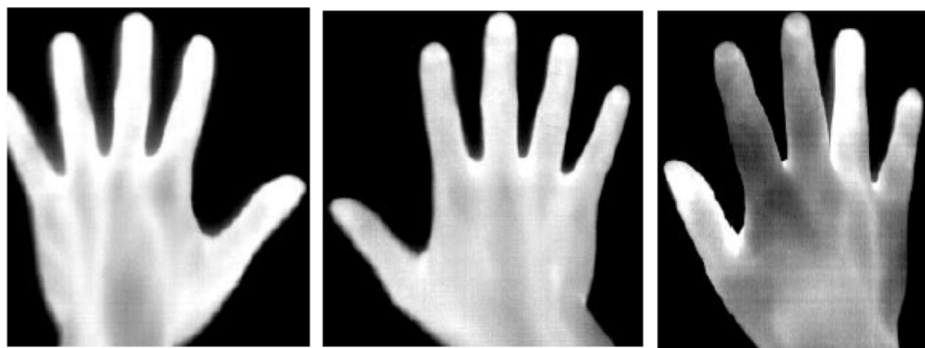


Figura 15 – Aquisição de imagem das veias da mão por meio de câmera térmica em ambiente com temperatura de 30° a 35° C

Fonte: (WANG e LEEDHAM, 2005).

Pode-se notar na figura acima que o discernimento das veias não é uma tarefa fácil quando em ambientes com temperaturas mais altas.

- Tratamento da Imagem

Após a captura da imagem da mão e suas veias por meio de uma câmera térmica, uma série de filtros são aplicados para tratar a imagem, diminuindo ruídos de alta frequência e manchas.

Em seguida é realizada a normalização da imagem para reduzir possíveis imperfeições geradas por ruídos do sensor e outros efeitos. A Figura 16 apresenta a imagem antes e depois de ser normalizada.

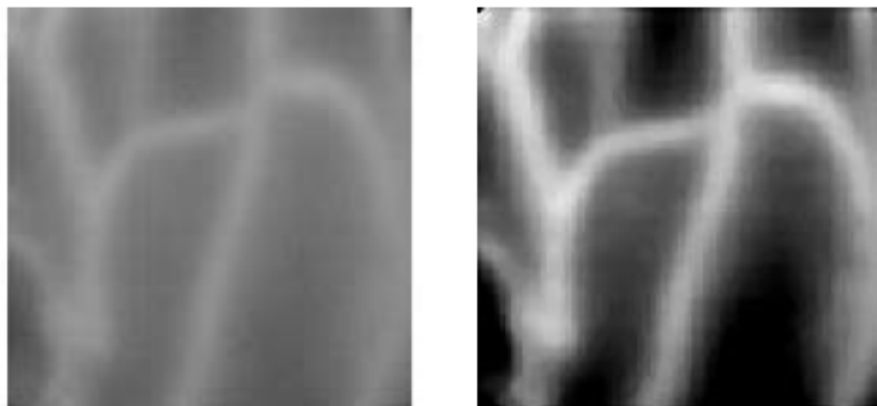


Figura 16 – Imagem das veias da mão antes e depois da normalização

Fonte: (WANG e LEEDHAM, 2005).

- Segmentação

Após a etapa de tratamento da imagem (redução de ruídos e normalização), a qualidade da imagem é melhorada, porém ainda não há uma diferenciação objetiva das veias da mão e demais imagens de fundo.

Portanto, nesta etapa é realizada a separação das veias da mão dos demais objetos da imagem, por meio de algoritmos de limiarização locais adaptativos, tornando a imagem discreta, ou seja, veias da mão em cor branca e demais regiões em cor preta, como pode ser visto na Figura 17 abaixo.

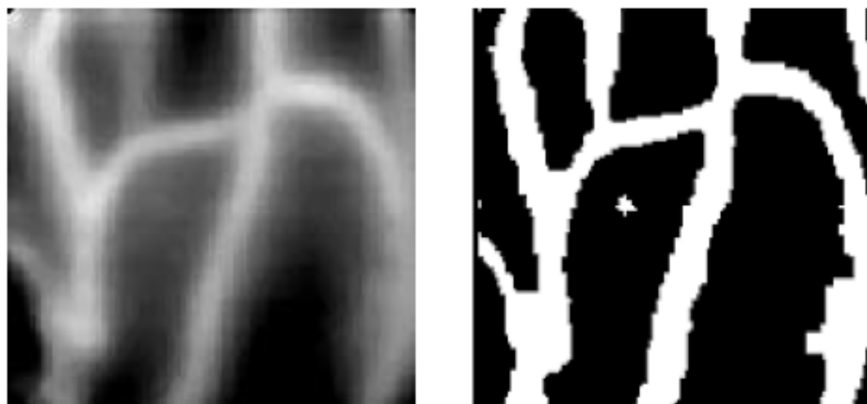


Figura 17 – Imagem das veias da mão antes e depois da segmentação

Fonte: (WANG e LEEDHAM, 2005).

- “*Skeletonization*”

À medida que o indivíduo cresce, o calibre das veias também aumentam, porém, para a identificação do indivíduo, apenas as formas dos padrões das veias são necessários. Ou seja, a informação sobre o calibre das veias é desnecessária.

Uma boa representação dos padrões das veias é obtida após a “*Skeletonization*”, ou seja, a aplicação de algoritmo de extração do padrão das veias em sua forma esquelética. A ideia é ter um padrão com linhas de calibre padronizado.

A seguir, pode ser visualizada a Figura 18 contendo o padrão de veias após a “*Skeletonization*”.



Figura 18 – Imagem das veias da mão antes e depois da *Skeletonization*

Fonte: (WANG e LEEDHAM, 2005).

- Comparação

A comparação é feita ao medir a distância “*Hausdorff*” de um segmento de linha entre pares de padrões de veias. A distância “*Hausdorff*” é uma medida natural para comparar a similaridade de formas usando-se a informação espacial da distância entre dois pontos definidos. Ela incorpora a informação estrutural da orientação de segmento de linha e associação linha-ponto, sendo assim efetiva para comparar duas formas compostas de um número de segmentos de curva.

Segundo (Wang e Leedham, 2005), nesta aplicação, os padrões de veias são divididos em um número de segmentos curvilíneos. Para cada segmento de curva

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.86/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

individual, alguns pontos são demarcados para representar o segmento de curva. Usando estes pontos demarcados, obtém-se um conjunto de segmentos de linha que representam a forma do padrão de veia. Assim, a linha de distância “Hausdorff” pode ser calculada para mensurar a similaridade entre dois padrões de veia.

7.2 CARACTERÍSTICAS TÉCNICAS

7.2.1 Universalidade

Todo ser humano possui um padrão de veias e artérias que são essenciais para a circulação de oxigênio e nutrientes para as extremidades do corpo. As veias, que estão sob a superfície da pele da palma da mão e dedos, existem em todas as pessoas (exceto aquelas que sofreram amputações ou má formação congênita) (WILSON, 2010).

No entanto, de acordo com (Jain et al, 2004), a característica universalidade é avaliada como mediana. Além de pessoas que possam não ter esses membros, acrescenta-se aqui outro grupo, o qual apresenta problemas de mobilidade dos membros em função de patologias, tais como artrite, artrose e paralisia. Doenças como diabetes, aterosclerose e tumores podem afetar o padrão das veias e torna-las mais finas ou mais grossas (Jain e Kumar, 2010).

7.2.2 Singularidade

Não há um consenso acadêmico acerca da unicidade das veias da mão.

Cientificamente ainda não foi provado que o padrão das veias da mão é único (Petitimbet et al, 2011) e (Nadort, 2007).

Segundo (Nadort, 2007), muitas fontes afirmam que os padrões de veias são uma propriedade única para cada indivíduo, tanto para a retina como para a mão. Pesquisas científicas em relação à singularidade das veias da mão ainda são esparsas.

Os estudos sobre o desenvolvimento do sistema vascular, associado ao arranjo espacial da rede de vasos sanguíneos pode trazer mais conhecimento acerca da probabilidade de o padrão de veias não ser o mesmo para dois indivíduos.

Segundo (Li e Jain, 2009), os padrões das veias da mão são formados por uma vasta rede de vasos sanguíneos debaixo da pele de uma pessoa e esses padrões das veias

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.87/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

são únicos mesmo para gêmeos idênticos (Li e Jain, 2009).

No entanto, seja em função da falta de estudos exaustivos, seja pelos problemas potenciais de captura e processamento da imagem, a característica singularidade é avaliada como mediana (Klokova, 2010) e (Jain et al, 2004).

7.2.3 Permanência

Alguns estudos (Jain e Kumar, 2010) e (Nadort, 2007) constataam que os padrões das veias são geralmente estáveis para adultos (20 - 50 anos de idade), mas em idades mais avançadas começam a apresentar problemas devido ao declínio na força dos ossos e músculos. Existem várias doenças, como diabetes, arteriosclerose ou tumores, que podem afetar os padrões de veias e torná-los grossos ou finos. Ademais, calor, frio, consumo de álcool e atividade física podem alterar o calibre das veias.

Para (Nadort, 2007), três são os processos que podem mudar o padrão das veias: 1) mudanças naturais relacionadas ao ciclo de vida do indivíduo; 2) mudanças naturais associadas a doenças; e 3) mudanças induzidas pelo uso de medicamentos ou por procedimentos cirúrgicos.

Abaixo, detalha-se cada um desses processos.

1) Ciclo de Vida: as mudanças no sistema vascular começam após o nascimento do indivíduo. As veias crescem acompanhando o crescimento do indivíduo como um todo, assim o comprimento das veias no corpo está em constante mudança nos primeiros 18 ou 20 anos da vida de uma pessoa. Durante a fase adulta, as mudanças são menos frequentes, e durante essa etapa (20 a 50 anos), o padrão das veias da mão praticamente não sofre qualquer alteração. Após essa faixa etária, os ossos e músculos começam a perder força, afetando de certa forma a circulação sanguínea, impactando no padrão das veias.

2) Doenças: o sistema vascular humano passa por constante renovação, por meio da renovação das células. Assim, algumas doenças como diabetes, hipertensão, arteriosclerose e tumores afetam algumas propriedades do sistema vascular que por sua vez alteram o calibre das veias.

3) Uso de medicamentos ou procedimentos cirúrgicos: o uso de medicamentos para doenças como o câncer pode alterar a formação do sistema vascular, já que o mesmo

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.88/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

atua no processo de mutação das células. Outra forma de modificar o sistema vascular se dá por meio de procedimento cirúrgico como o alargamento da coronária para uma melhor vazão do sangue em todo o corpo. Também, as microcirurgias de varizes impactam no sistema vascular. Além de que, procedimentos locais na mão podem mover as veias de lugar, alterando a leitura.

7.2.4 Coletabilidade

Existem algumas restrições quanto ao ambiente do local da coleta da biometria. Como os equipamentos de aquisição são baseados em tecnologia de infravermelho, a temperatura local pode inviabilizar a correta coleta da imagem das veias da mão.

A coleta também pode ser difícil em proximidade a outras fontes emissoras de calor, como aquecedores e exaustores (Jain et al, 2004). A presença de pelos, cicatrizes e verrugas podem influenciar a captura (Kumar e Prathyusha, 2009).

Recentemente, a Fujitsu colocou no mercado um novo leitor conhecido como *PalmSecure* que apresenta várias melhorias em relação aos leitores antigos. O novo leitor é higiênico, pois não requer contato físico e o sensor é de tamanho reduzido.

A Fujitsu recomenda evitar contato direto com luz solar, assim como foco direto de lâmpadas incandescentes e alógenas³⁵. Tal fato pode ser interpretado como uma dificuldade de coletar a biometria em ambiente externo ou sob condições anormais de temperatura, luminosidade e umidade.

O forte fator infravermelho presente na luz solar limita o uso externo (Kumar e Prathyusha, 2009).

Algumas tintas de tatuagem podem também absorver a luz infravermelha, prejudicando a coleta (Modi, 2011).

A característica coletabilidade recebe avaliação média segundo (Klokova, 2010) e (Jain et al, 2004).

7.2.5 Desempenho

A Fujitsu alega que, utilizando uma base de 140.000 mãos, atingiu uma Taxa de Falsa

³⁵ http://www.fujitsu.com/global/Images/PalmSecure_Datasheet.pdf

Aceitação (FAR) de 0,00008% para uma Taxa de Falsa Rejeição (FRR) de 0,01%, o que significa que 1 em cada 10.000 pessoas não será reconhecida pelo sistema, enquanto 1 em cada 1.250.000 será reconhecida falsamente como outra pessoa³⁶.

De acordo com José Alberto Canedo³⁷, as informações disponibilizadas pela Fujitsu podem estar superestimadas já que inexistem dados e equipamentos de outras empresas para fins de teste e comparação.

(Nadort, 2007) comenta sobre o tratamento "caixa preta" da indústria da biometria e que contrário à atitude de segredo das companhias como forma de proteção contra impostores e fraudes, seus sistemas podem se beneficiar de uma abordagem aberta de inspeção, análise, crítica e melhora.

(Yuksel et al, 2010) concordam que se trata de um revés ao avanço da biometria da veia da mão a falta de bases de dados abertas, trazendo ausência de resultados reproduzíveis.

Essa característica é avaliada como mediana (Klokoova, 2010) e (Jain et al, 2004).

7.2.6 Aceitabilidade

O sistema de reconhecimento com base nas veias da mão não necessita de contato direto, podendo ser percebido como mais higiênico e menos invasivo. Mas o público, em geral, poderia, eventualmente, considerar os raios infravermelhos como perigosos e invasivos.

Segundo José Alberto Canedo³⁸, não há um consenso se esta biometria é mais aceitável que as outras existentes.

De acordo com (Jain e Kumar, 2010), a leitura distante do aparelho geralmente agrada o usuário.

(Hartung, 2012) defende a alta aceitabilidade dizendo que esta biometria não está relacionada à investigação criminal, e se referiu ao sucesso na região Extremo Oriente asiático.

Essa característica é avaliada como mediana (Klokoova, 2010) e (Jain et al, 2004).

³⁶ <http://www.fujitsu.com/br/news/pr/2006/20060310.html>

³⁷ <http://www.forumbiometria.com/artigos/36-geral/48-biometria-das-veias-da-mao-hand-veins.html>

³⁸ <http://www.forumbiometria.com/artigos/36-geral/48-biometria-das-veias-da-mao-hand-veins.html>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.90/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

7.2.7 Resistência à fraude

Esta é a característica que, comparada às outras biometrias, pode ser considerada superior, principalmente por estar dentro do corpo da pessoa. Por outro lado, pelo fato da tecnologia não estar disseminada, após sua popularização, pode apresentar possibilidades de fraudes³⁹.

Além de inacessíveis, seja pelo contato ou visualização, as veias formam uma complexa rede, dificultando a cópia fraudulenta (Guru et al, 2011).

Segundo (Nadort, 2007), a não utilização de equipamentos de aquisição com detecção de vivacidade, permite que padrões de veias desenhados com tinta em papel possam burlar o sistema de reconhecimento. Para o autor, grandes avanços na robustez da prevenção contra impostores ainda não foram atingidos devido ao sigilo de tecnologia.

De acordo com (Klokoova, 2010) e (Jain et al, 2004), essa característica é avaliada como alta em virtude da complexidade dos padrões desta biometria associado ao fato de acesso ao padrão das veias (subcutânea) e, conseqüentemente, sua capacidade de resistir à fraude.

7.3 ESTIMATIVA DE CUSTO

A popularização do uso de sistema de reconhecimento biométrico baseado nas veias da mão ainda depende de seu custo. Estima-se que o leitor de veias da mão custe aproximadamente U\$1.000, enquanto o leitor de impressões digitais custa em torno de U\$30 a U\$100⁴⁰.

Não há um sistema em larga escala de biometria vascular, possivelmente devido ao custo do sistema e falta de estudos em grande escala (Jain e Kumar, 2010).

Outro fator determinante no elevado custo da biometria é a posse da patente da tecnologia pela empresa Fujitsu.

7.4 CARACTERÍSTICAS DA COLETA

7.4.1 Idade inicial

³⁹ <http://www.forumbiometria.com/artigos/36-geral/48-biometria-das-veias-da-mao-hand-veins.html>

⁴⁰ <http://www.forumbiometria.com/artigos/36-geral/48-biometria-das-veias-da-mao-hand-veins.html>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.91/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Informações comerciais da empresa Fujitsu apontam que a partir dos 5 anos já é possível fazer a coleta de 100% das pessoas. A Fujitsu informa que o uso do dispositivo *PalmSecure* independe de idade⁴¹.

Um distrito escolar da Flórida tem avaliado positivamente a implementação do dispositivo de leitura de veias da mão, *PalmSecure*, da Fujitsu, para identificação de alunos na fila do almoço. Cinquenta mil estudantes estão cadastrados, já inclusos os alunos da primeira série, na média de 6 e 7 anos⁴².

7.4.2 Tamanho do arquivo gerado

Segundo informações comerciais da FUJITSU, o tamanho do arquivo do *template* gerado é de 800 bytes⁴³.

De acordo com o fabricante Hitachi, o *template* gerado pelos sensores possui um tamanho de 400 bytes (Edgington, 2007).

7.4.3 Tempo de coleta

Segundo o trabalho publicado por (Nadort, 2007), o tempo de coleta dos traços da veia da mão demora em média 66.8 segundos utilizando os equipamentos da Fujitsu e 38.4 com os equipamentos da Hitachi.

7.5 ALGORITMOS DE RECONHECIMENTO

A avaliação de quão bom um algoritmo é para realizar a identificação de uma determinada biometria depende de qual característica se está analisando: EER, FRR, FAR, velocidade de comparação, velocidade de cadastramento, tamanho do banco de dados, dentre outras.

Para as veias da mão, ainda não há competições que promovam a avaliação de algoritmos de reconhecimento.

⁴¹ http://www.fujitsu.com/pt/Images/Palm_Secure.pdf

⁴² <http://www.usatoday.com/story/news/nation/2012/11/25/palm-scanners-technology-schools/1726175/>

⁴³ http://www.fujitsu.com/downloads/COMP/ffna/palm-vein/PCSD_casestudy.pdf

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.92/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

7.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Acredita-se que não haja influências restritivas ao trabalho ou à cultura do brasileiro em relação à utilização das veias da mão como biometria para verificação.

Segundo (Modi, 2011), trabalhadores que atuam em contato com carvão ou fuligem podem ter a imagem de suas veias da mão impactadas negativamente em virtude da presença de substâncias que absorvem a iluminação infravermelho.

Em 2010, o Bradesco decidiu expandir o uso da biometria nos seus caixas eletrônicos para reforçar a segurança durante as transações⁴⁴, com previsão de investimentos, em de 250 milhões de reais para compra de oito mil terminais com sistema *PalmSecure* (Fujitsu).

Segundo o diretor executivo do Bradesco, em 2013, 13 dos 27 milhões de correntistas do banco já tinham suas biometrias de veias da palma da mão cadastradas⁴⁵.

7.7 UTILIZAÇÃO EM OUTROS PAÍSES

Até a data de hoje, não existe nenhuma implementação dessa biometria em um sistema de identificação biométrico civil de grande escala.

Em relação aos fabricantes da tecnologia de reconhecimento das veias da mão, a empresa Fujitsu tem amplo domínio do mercado, incluindo várias patentes, dispositivos e sistemas próprios. O sistema *PalmSecure* é o mais conhecido comercialmente, sendo inclusive utilizado pelo banco Bradesco em seu sistema biométrico no Brasil.

Em 2007, a rede de saúde *Carolinas HealthCare System* implementou o dispositivo *PalmSecure*, e em 2011 tinha 1,5 milhão de pacientes cadastrados e identificados⁴⁶.

O sistema de identificação de pacientes *PatientSecure*⁴⁷, patente de HT Systems, foi implementado em 2007 e hoje foi adotado por mais de 250 hospitais e instalações de saúde e contempla mais de 5 milhões de pacientes cadastrados, com 20 mil autenticações em média por dia.

Este sistema biométrico foi implementado por instituições financeiras no Japão a partir

⁴⁴<http://cio.com.br/gestao/2010/01/20/seguranca-da-informacao-bradesco-investe-r-250-milhoes-em-biometria/>

⁴⁵<http://computerworld.com.br/seguranca/2013/03/14/bradesco-testa-biometria-no-internet-banking-para-substituicao-de-senhas/>

⁴⁶ <http://www.emrandehrnews.com/tag/carolinas-healthcare-system/>

⁴⁷ <http://www.patientsecure.com/>

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.93/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

de 2004, incluindo o terceiro maior banco, o *Tokyo-Mitsubishi*. Usuários do banco *gaki Kyoritsu* podem acessar máquinas de saque sem cartão ou número de identificação.

A tecnologia de reconhecimento de veias é usada e aceita em várias instâncias neste país: escolas, apartamentos, aeroportos (Wilson, 2011).

7.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

A biometria das veias da mão é indicada para verificação (1:1), segundo os testes realizados pela empresa Fujitsu, detentora da patente de reconhecimento.

Entretanto, devido à falta de popularização da tecnologia, a comercialização de produtos de outros fabricantes e a falta de competições abertas, como as realizadas pelo NIST, fazem com que a tecnologia não seja considerada madura o suficiente para o processo de identificação (1:N) em um projeto de grande escala.

7.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

A tecnologia de reconhecimento das veias da mão apresenta indefinições quanto às vantagens de alta precisão e resistência à fraude, já que as informações e tecnologias existentes são praticamente oriundas da detentora da patente e fornecedora dos equipamentos. Contudo, é uma biometria não invasiva que proporciona grande aceitabilidade. Dentre os pontos negativos podem-se destacar a permanência e o alto custo da tecnologia, que são dois fatores cruciais no projeto RIC.

Devido a insegurança das informações e tecnologias, adicionada à baixa permanência e o alto custo, o reconhecimento das veias da mão não é aplicável ao projeto RIC.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.94/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

8 VOZ

8.1 INTRODUÇÃO

As cavidades vocais como o nariz e a garganta, além do tamanho e forma das cordas vocais, são características físicas presumidamente únicas. O movimento da mandíbula e dos lábios, o sotaque adquirido e as influências ambientais são componentes comportamentais que não são replicáveis, com total fidelidade, por dois diferentes indivíduos. O reconhecimento da fala, também conhecido como “biometria da fala” ou “reconhecimento da voz”, é baseado na premissa de unicidade dos componentes físicos e comportamentais acima citados.

De acordo com (Sá et al, 2012):

Os aspectos comuns de comportamento dos indivíduos expressam características adquiridas do grupo regional e social em que tiveram a sua formação cultural. Assim, os traços linguísticos de um falante também são marcados pelo ambiente de sua formação e crescimento. Portanto, ao se comunicar através da fala, o indivíduo expressa o seu pensamento de acordo com a sistemática de suas ideias, do seu conhecimento, dos padrões de comportamento adquiridos e de atitudes que fornecem pistas do seu perfil e ambiente de origem.

O reconhecimento da voz pelo ser humano pode ser efetuado mesmo em condições adversas, com diferentes tipos de distorções e limitações do sinal acústico (Figueiredo, 1994).

Outra modalidade de reconhecimento automático que faz uso da voz é o “Reconhecimento Automatizado do Discurso” – “ASR”. O ASR é geralmente confundido com o reconhecimento da fala. No entanto, ele é usado para converter a voz em um texto correspondente e envolve o processo da transcrição, enquanto que o reconhecimento da fala é usado para autenticar um usuário a partir das características da voz sem preocupar-se com o conteúdo do discurso. O ASR não se preocupa com quem está falando, mas sim em decifrar o que está sendo dito.

O reconhecimento da voz é considerado uma tecnologia biométrica pelas seguintes razões.

- a) Ela é um sinal que humanos aprendem a emitir naturalmente;
- b) O reconhecimento da voz é usado implicitamente no dia-a-dia;
- c) A ubiquidade (presença em todos os lugares) da infraestrutura de

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.95/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

telecomunicações torna possível a captação da voz de forma bastante simples embora isso seja feito sem respeitar critérios de coleta que são necessários, ainda hoje, para o êxito da identificação.

O reconhecimento da fala é uma área ativa de pesquisa com grande potencial comercial, mas ainda é uma tecnologia com limitações para adoção no mundo real. Os sistemas de verificação de voz superam os sistemas de identificação de voz, mas ambos são objetos de estudo em pesquisas (Sá et al, 2012).

Durante o processo da fala, são transmitidas, além da mensagem que o locutor deseja levar, informações pessoais, intrínsecas a uma determinada pessoa. Essas informações extras permitem conhecer a formação linguística e cultural do locutor, sua origem regional e social, além de sua identidade física e humor.

Diante disso, a voz é considerada exemplo de identificação pessoal biométrica.

ETAPAS DO PROCESSO

O processo básico de identificação pode ser descrito da seguinte forma.

- **Captura:** o usuário fala num microfone e dita uma frase previamente selecionada (dependente) ou randômica (independente). Este processo geralmente é repetido algumas vezes para se construir um perfil da voz.

- **Extração:** o equipamento biométrico extrai o sinal único da voz e então um *template* é criado.

- **Comparação:** a verificação um-para-um (1:1) é o método preferencial. O usuário fala em um microfone; o novo exemplo de voz é então comparado com o *template* armazenado.

O reconhecimento da voz é utilizado tanto para identificação como para verificação. Pesquisas em relação ao reconhecimento da fala tem como base pesquisas em reconhecimento de padrões e a literatura acadêmica geralmente utiliza termos como “treinamento” e “teste” para descrever o processo de cadastramento e reconhecimento, respectivamente. Os sistemas de reconhecimento da fala são categorizados com base nos tipos das amostras de discurso que um usuário produz durante as etapas de cadastramento e reconhecimento (figura abaixo): texto-dependente, texto-solicitado e texto-independente (Modi, 2011).

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.96/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

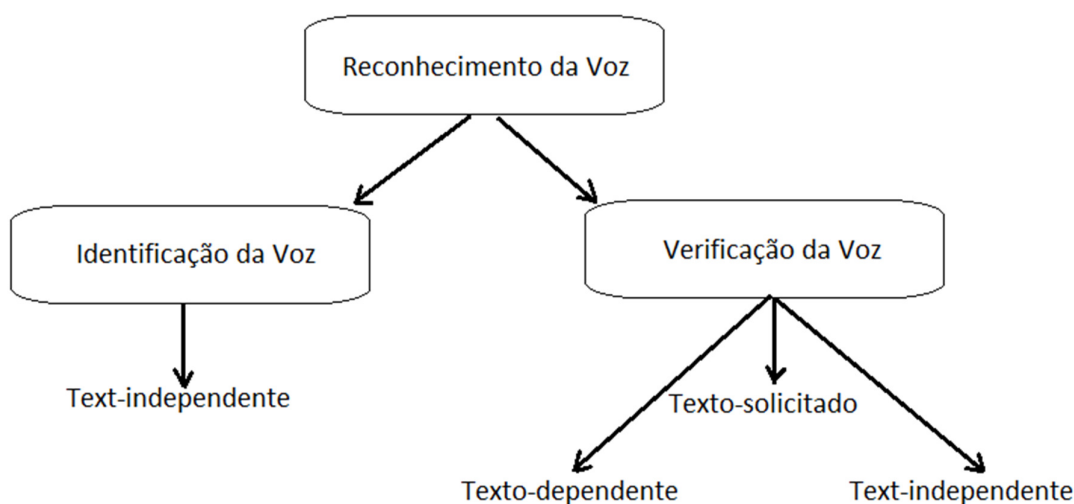


Figura 19 – Tipos de sistemas de reconhecimento da fala (voz).

- i) **Texto-Dependente:** os sistemas com texto-dependente têm conhecimento explícito de palavras e frases que o usuário irá falar e a ordem em que elas serão faladas, o que permanece o mesmo para cada transação. Isso é uma palavra, número de conta, ou palavra secreta que é utilizada durante o cadastramento. A maioria dos sistemas comerciais disponíveis se encaixam nesta categoria principalmente se eles são robustos a interferências ambientais e geram poucos erros.
- ii) **Texto-Solicitado:** nesse tipo de sistema o usuário é orientado a falar uma palavra ou frase específica, mas a ordem em que ela é falada é sempre diferente. É uma extensão do sistema de texto-dependente porque o sistema tem prévio conhecimento das possíveis palavras que serão ditas pelo usuário. Cada sistema também requer que o usuário cadastre uma amostra grande de discurso para garantir que cada componente possível do discurso seja gravado. Esse é o tipo de sistema que permite a melhor proteção contra ataques de *replay*, quando o usuário utiliza amostra de uma voz gravada. O uso de sistema do tipo texto-solicitado é restrito a aplicações para clientes comuns.
- iii) **Texto-Independente:** em sistemas do tipo texto-independente, o usuário não fica restrito a um rol de palavras ou frases específicas. O sistema não tem

pré-conhecimento da amostra de discurso - a amostra de cadastramento e reconhecimento podem ser completamente diferentes. Esse é um problema bem mais difícil de resolver já que ele requer características de comparação de duas amostras diferentes que podem não ter nem mesmo duas sílabas em comum. Os sistemas de texto-independente têm tradicionalmente ganhado mais atenção por parte das agências de inteligência e aplicações governamentais para identificar pessoas de interesse utilizando sinais de telecomunicações. Esses sistemas podem ser usados para identificação de voz (isto é, promove comparação sem solicitar a identidade do indivíduo), mas as taxas de erro são tipicamente mais altas que 10% dependendo do nível de barulho ao fundo.

Na fase de comparação para sistemas do tipo texto-solicitado e texto-independente, não é possível criar vetores de características para cada possível ocorrência em um sinal de voz. Nestes casos, são utilizados modelos estocásticos para comparar dois sinais de voz. Modelos estocásticos formulam um problema de comparação de padrões com um teste hipotético (*likelihood ratio* – *LR*), verificando a similaridade dos modelos cadastrado e verificado. Se a probabilidade é maior que um determinado limiar (*threshold*), então o reconhecimento é informado.

Empiricamente, *Gaussian Mixture models* (GMM) apresentaram melhores resultados para sistemas tipo texto-independente. Por outro lado, *Hidden Markov models* (HMM) têm a capacidade de incorporar informações disponíveis em sistemas do tipo texto-dependente e texto-solicitado.

Modelos do tipo HMM são mais difíceis de serem implementados quando comparados aos GMM e promovem melhores resultados em sistemas do tipo texto dependente. Resultados do NIST *Speaker Recognition Evaluation* (SER) apontam que não há grande diferença entre HMM e o GMM para sistemas do tipo texto-independente (Modi, 2011).

8.2 CARACTERÍSTICAS TÉCNICAS

8.2.1 Universalidade

Segundo dados do (Censo IBGE, 2010), no Brasil 5,5% da população entre 0 e 64

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.98/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

anos de idade possuem algum grau de deficiência auditiva. Sabe-se da relação entre surdez e mudez. Esta relação é apontada em diversos trabalhos científicos das áreas de otorrinolaringologia e fonoaudiologia. (Padovani e Teixeira, 2005) comentam sobre a impossibilidade do surdo em falar, uma vez que não ouve as palavras e então não é naturalmente vocalizado. Sendo assim, a identificação pela voz nestes casos torna-se praticamente impossível.

De acordo com (Jain et al, 2004), a universalidade da voz é avaliada como média.

8.2.2 Singularidade

Cada indivíduo possui características próprias durante a produção de sons vocais. Um conjunto de fatores dão caráter único a cada indivíduo. Esses se devem aos articuladores, ou seja, estruturas flexíveis que alteram a característica do som produzido, dentre eles a língua como principal.

A imitação de voz não é eficaz, pois o som produzido não é analisado por programas de reconhecimento automático da mesma forma com que humanos o fazem. Variáveis físicas como a frequência do som podem ser verificadas por *softwares* específicos para tal análise.

Segundo (Jain et al, 2004), a característica singularidade é avaliada como baixa.

8.2.3 Permanência

(Jain et al, 2004) classifica a permanência da voz como baixa uma vez que esta pode sofrer alterações ao longo da vida.

Em publicação da sociedade brasileira de fonoaudiologia, (Azevedo et al, 2009) informa que há interferência de atividades profissionais na saúde vocal e profissionais como professores. Alterações nos músculos que trabalham na produção da voz podem ocorrer também por conta de nódulos na tireoide, segundo o Instituto Brasileiro de Controle de Câncer. Tais afirmações endossam a classificação dada por Anil Jain a este quesito.

8.2.4 Coletabilidade

A tecnologia de reconhecimento de voz permite a coleta de forma relativamente

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.99/125
--------------------	---------------------	---	------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

simples. A captura do som da voz é realizada posicionando-se o usuário em frente a um aparelho captador (um microfone, por exemplo) e, em seguida, o usuário deverá pronunciar uma frase previamente selecionada ou ainda uma frase qualquer. Este processo precisa ser repetido diversas vezes objetivando a construção de um modelo. Deve-se garantir que o usuário fale em um tempo apropriado e em voz clara.

Recomenda-se que, durante o reconhecimento ou cadastramento da biometria, o usuário esteja com sua voz em condições normais (ausência de faringite, gripes, resfriados e até mesmo alteração emocional), evitando cadastramento incorreto ou falha na identificação ou autenticação.

Observa-se que na coleta da voz torna-se necessária a presença de um agente humano.

A característica é avaliada por (Jain et al, 2004) como mediana.

8.2.5 Desempenho

Segundo (Costa et al, 2006):

Os pontos fortes da tecnologia de autenticação biométrica no padrão de voz são:

- A voz é uma biometria usada instintivamente pelas pessoas para autenticação mútua.
- Sistemas com infraestrutura telefônica constituem o principal alvo do reconhecimento de voz. A fala com o objetivo único de autenticação (autenticação ativa), pode ser um tanto quanto antinatural, mas em situações em que o usuário já tem mesmo de falar, o protocolo de autenticação se torna passivo, amigável e não intrusivo.
- Esta tecnologia utiliza dispositivos baratos, e além disso é facilmente desenvolvida sobre uma infraestrutura já existente e amplamente espalhada, como o sistema telefônico.
- Permite protocolos de autenticação de segurança incremental.
 - Quando maior confiança é necessária, o sistema pode suportar mais dados de voz.
 - Pode ser utilizado um protocolo de biometria conversacional, combinado com verificação de conhecimento.
 - O protocolo pode verificar a identidade continuamente durante a conversação.
- Em aplicações de texto independente e aplicações conversacionais, os

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Prováveis de Utilização no RIC.docx	Pág.100/125
--------------------	---------------------	---	-------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

usuários não necessitam de um processo separado de autenticação, o que torna o processo totalmente integrado.

Quanto aos pontos fracos, podemos citar:

- É possível a imitação por pessoas habilidosas ou a utilização de gravações da voz do usuário legítimo para fraudar o sistema. Além disso, existem sistemas de síntese que podem ser treinados para imitar a voz de pessoas.
- A tecnologia *text-to-speech* torna possível a criação de identidades não existentes, em sistemas de registro e autenticação remotos.
- A qualidade do sinal de áudio é suscetível ao ruído do ambiente. Além disso, são introduzidas distorções na captação do sinal pelo microfone e na transmissão do sinal através do canal.
- O padrão de voz é bastante frágil, pois pode ser alterado pelo estado do usuário (saúde, emoção, pressa, sono, preguiça, entre outros).

A seguir encontra-se uma figura com taxas aproximadas de FAR e FRR para algumas biometrias, dentre elas a voz.

Pode-se verificar que os valores aproximados para as taxas FRR e FAR, respectivamente, são 5-10% e 2-5% para voz. Nota-se que são taxas elevadas em relação às outras biometrias, como mostra a figura abaixo.

Biometric trait	Test	Test conditions	False reject rate	False accept rate
Fingerprint	FVC 2006 [9]	Heterogeneous population including manual workers and elderly people	2.2%	2.2%
	FpVTE 2003 [10]	US government operational data	0.1%	1%
Face	FRVT 2006 [11]	Controlled illumination, high resolution	0.8%–1.6%	0.1%
Voice	NIST 2004 [12]	Text independent, multi-lingual	5–10%	2–5%
Iris	ICE 2006 [11]	Controlled illumination, broad-quality range	1.1%–1.4%	0.1%

Figura 20 – Taxas FAR e FRR para a biometria voz.

A característica desempenho é avaliada como baixa (KLOKOVA, 2010 e JAIN, 2004).

8.2.6 Aceitabilidade

Trata-se da característica biométrica melhor avaliada no caso da voz, haja vista ser um dos métodos de identificação biométricos menos invasivos e que dispensa o contato com qualquer dispositivo.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.101/125
--------------------	---------------------	---	-------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.

É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Segundo (Klokova, 2010) e (Jain et al, 2004), a característica aceitabilidade é avaliada como alta.

8.2.7 Resistência à fraude

De acordo com (Klokova, 2010) e (Jain et al, 2004), a característica recebe nota baixa, mostrando-se mais susceptível a fraudes.

Gravações de alta qualidade são consideradas as formas mais utilizadas para tentar burlar um sistema de reconhecimento de voz. Vale ressaltar que para evitar esse tipo de fraude, normalmente são utilizadas conversas diferentes, já que assim as gravações não teriam sentido (Geradts e Sommer, 2006).

8.3 ESTIMATIVA DE CUSTO

Essa informação não foi encontrada na bibliografia ora apresentada.

8.4 CARACTERÍSTICAS DA COLETA

8.4.1 Idade inicial

Os defensores da análise espectrográfica ressaltam que o posicionamento dos articuladores (dentes, língua e lábios) torna-se tão habitual que o orador não pode mudar significativamente seus padrões de voz, tornando, assim, as características únicas da voz de cada indivíduo imutável. No entanto, até que a pessoa amadureça fisicamente e linguisticamente, as mudanças nos padrões de voz irão ocorrer. Assim, amostras de voz de crianças devem ser realizadas frequentemente.

8.4.2 Tamanho do arquivo gerado

De acordo com Simson L. Garfinkel⁴⁸, o tamanho do *template* gerado para a biometria voz é de 70 kb a 80 kb.

8.4.3 Tempo de coleta

Para a biometria da voz, o tempo de coleta é muito dependente do tipo de

⁴⁸ http://simson.net/ref/2004/csg357/handouts/L10_biometrics.ppt

reconhecimento a ser utilizado (texto-solicitado ou texto-independente). Além disso, depende da quantidade de palavras ou frases a serem faladas a fim de permitir a identificação.

Segundo informações do Sindicato das Empresas de Sistemas Eletrônicos do Estado de São Paulo, SIESE-SP, o banco *Tatra Bank*, da Eslováquia, faz a verificação de um cliente em sua base num intervalo de tempo entre dez e quinze 15 segundos de conversa normal, numa amostra de aproximadamente de 30.000 clientes⁴⁹

8.5 ALGORITMOS DE RECONHECIMENTO

O grupo de estudos da voz (*The Speech Group*) no NIST tem desempenhado papel crucial na avaliação do atual estado da arte em detecção em sistemas de texto-independente e identificando áreas desafiadoras em suas competições de reconhecimento da fala (*Speaker Recognition Evaluation – SER*), que ocorrem desde 1996. O principal foco de cada SER é em relação à detecção da fala (voz).

A performance dos algoritmos que participam da SER é calculada em termos de uma função de custos cujos parâmetros de detecção perdida e falso alarme são fixados pelo NIST. A detecção perdida tem um custo muito alto quando comparada ao falso alarme.

Cada SER tem mostrado uma redução na taxa de erro equivalente (EER) em relação à competição anterior, mesmo com níveis de dificuldades maiores. A SER de 2008 apresentou EER menores que 2%.

Em 2003, a *Netherlands Forensic Institute* (NFI) e a *Netherlands Organization for Applied Scientific Research* (TNO) publicaram um relatório sobre sistemas de detecção da fala, no qual 15 sistemas foram avaliados. Os valores de EER apresentados variaram de 12,1% a 35%⁵⁰.

Em 2004, o (IBG, 2005) conduziu um teste de verificação de voz em três sistemas comercialmente disponíveis projetados para aplicações de autenticação de endereços relacionados a instituições financeiras. No total, 219 indivíduos participaram do teste, por meio de linhas telefônicas fixas e móveis (celulares). Foram cadastrados 20 *templates* de usuários para gerar impostores. Em geral, o sistema se comportou melhor para linhas

⁴⁹ http://www.bbc.co.uk/portuguese/noticias/2013/11/131112_tecnologia_reconhecimento_voz_fn.shtml

⁵⁰ VAN LEEUWEN, D. et al. Results of the 2003 NFI-TNO forensic speaker recognition evaluation. In: Proc. Odyssey 2004 Speaker and Language recognition workshop, ISCA. 2004. p. 75-82

fixas quando comparado a celulares. Os menores valores de FMR e FNMR verificados foram, respectivamente, 0,586% e 0,800% (Modi, 2011).

8.6 CARACTERÍSTICAS RELATIVAS À POPULAÇÃO BRASILEIRA

Acredita-se que não haja influências restritivas ao trabalho ou da cultura do brasileiro em relação à utilização da voz como biometria para verificação. A biometria da voz é indicada para verificação num grupo específico, com amostra reduzida, que possibilite a autenticação do usuário sem a necessidade da presença física.

8.7 UTILIZAÇÃO EM OUTROS PAÍSES

Até a data de hoje, não existe nenhuma implementação dessa biometria em um sistema de identificação biométrico de grande escala.

Algumas empresas como *Visa* e *Ebay* já adotam a biometria voz para autenticar o usuário para realizar alguns serviços. Como exemplo, *Visa* permite a autenticação por voz para a realização de *reset* de senha em sistemas automatizados e consultas de compras realizadas. Uma empresa de referência em sistemas de reconhecimento da voz em âmbito mundial é a espanhola *Agnitio*⁵¹, sendo o *Kivox360* o produto referência no mercado.

8.8 UTILIZAÇÃO NA IDENTIFICAÇÃO E/OU VERIFICAÇÃO

Segundo (Jain e Kumar, 2010), a biometria da voz é usada principalmente no modo verificação (1:1) em virtude da baixa permanência da biometria (influências do timbre e intensidade) e baixa precisão no reconhecimento da voz.

8.9 RECOMENDAÇÃO DE UTILIZAÇÃO NO PROGRAMA RIC

A tecnologia de reconhecimento da biometria da voz não é a mais segura quando comparada a outras biometrias. Além disso, a voz humana muda com o tempo. Desta forma, o *template* cadastrado de um usuário jovem possivelmente não poderá ser comparado com sua voz quando adulto. Para contornar tal problema, a frequência de

⁵¹ <http://www.agnitio-corp.com/>

atualizações cadastrais será alta, o que é inviável para um projeto em larga escala.

Desta forma, esta biometria não é recomendada para o programa RIC.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.105/125
--------------------	---------------------	---	--------------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

9 CONCLUSÃO

Foram realizados estudos bibliográficos detalhados nas seis biometrias previamente definidas como as mais promissoras, ou seja, assinatura, face, impressão digital, íris, veias da mão e voz.

Dessas seis biometrias supracitadas duas delas apresentam, conforme pode ser verificado no texto e observado inclusive visualmente nos mapas mentais deste relatório, os melhores desempenhos nos diversos critérios utilizados para classificação. São elas: íris e impressão digital.

A biometria impressão digital embora tenha bom desempenho em relação ao quesito precisão, em função da grande escala do projeto (200 milhões de brasileiros) pode apresentar erros de falsa aceitação e falsa rejeição elevados, além de cerca de 21,1% da população brasileira (cerca de 42 milhões) ser potencial a apresentar danos e desgastes da referida biometria. Ademais, a coleta desta biometria exige preparo e treinamento específicos para minimizar erros que podem chegar a até 5%.

Porém ressalta-se que há, além de uma cultura já estabelecida no país, um legado que utiliza basicamente a impressão digital na identificação civil.

Portanto, visando garantir a inclusão de toda a população brasileira, bem como manter a não-duplicação (de-duplicação) de dados do banco nacional e também unicidade da identificação civil com elevada precisão, faz-se necessário contemplar o Programa de Identidade Civil Brasileiro (RIC) com uma biometria adicional, a qual deve ser extremamente precisa e inclusiva.

De todas as biometrias elencadas, a mais promissora, que contempla os quesitos supracitados e que tem sido utilizada em grandes projetos de identificação civil mundial é a íris.

A íris apresenta uma avaliação da característica universalidade extremamente elevada, já que a maioria das pessoas possuem senão as duas íris, pelo menos uma delas. Neste sentido, a percentagem potencial de inexistência das duas íris (anirídia) é de 0,0018% na população mundial. Ou seja, considerando a população brasileira de 200 milhões, ter-se-ia 3.600 pessoas potenciais de não apresentarem as duas íris. Nestes casos utilizar-se-ia apenas a impressão digital.

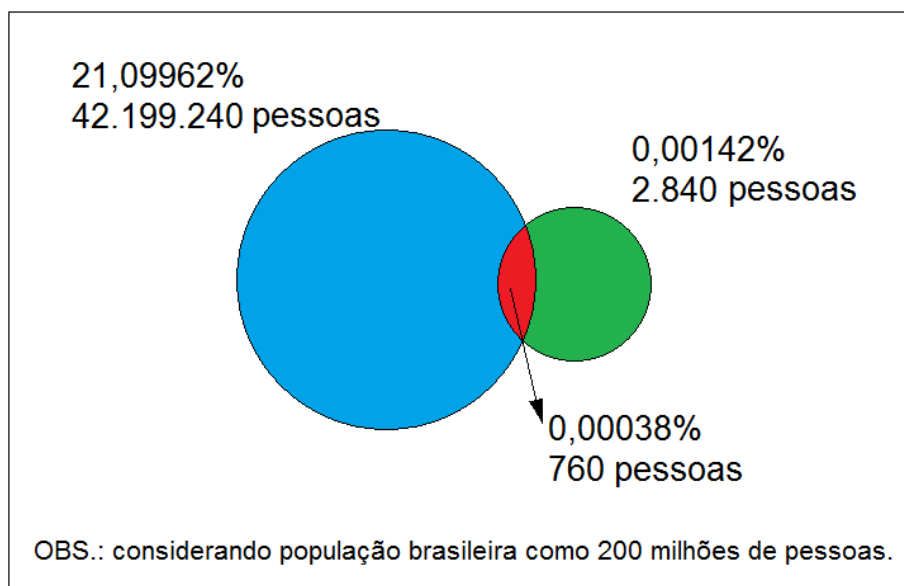
Considerando-se ainda que o percentual de possíveis não portadores de impressões

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.106/125
--------------------	---------------------	---	-------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

digitais é de 21,1%, ou seja, 42,2 milhões de pessoas, ao se combinar as duas biometrias, íris e impressão digital, o percentual de pessoas que potencialmente não teriam ambas as biometrias seria de 0,00038%, ou seja, apenas 760 pessoas. O cálculo, baseado em probabilidades, foi realizado considerando-se que $P(A \cap B) = P(A) \cdot P(B)$, ou seja, a probabilidade da ocorrência da interseção de dois conjuntos é exatamente a multiplicação das probabilidades de ocorrência de cada um dos conjuntos, conforme Figura 21 abaixo.



- potenciais não portadores de impressão digital
- potenciais não portadores de impressão digital e íris
- potenciais não portadores de íris (aniridia)

Figura 21 – Percentual de brasileiros potenciais não portadores de impressão digital e íris.

Corroborando a avaliação positiva da biometria íris, destaca-se, ainda, a elevadíssima precisão em relação a erros de falsa aceitação e falsa rejeição utilizando-se duas íris.

Além disso, a coleta da íris é bastante simples, rápida e não necessita de treinamento específico do coletor.

Outra característica a ser salientada é o custo de aquisição da íris que até a alguns anos atrás era um fator limitante. Atualmente, com a queda da patente em 2011 e a utilização da íris no Programa de identificação civil da Índia, Indonésia e México, esse

custo vem decrescendo vertiginosamente.

Considerando-se que o custo unitário de implantação da impressão digital como biometria de identificação varia de R\$ 5,98 a R\$ 6,49, e que o custo unitário do acréscimo da íris também como biometria para identificação varia de R\$ 1,16 a R\$ 1,27, tem-se que o percentual de acréscimo da íris é de apenas 19,4% a 19,6%. Tal custo pode ser interpretado como razoável, levando-se em consideração que a utilização da íris aumenta consideravelmente a inclusão de indivíduos no programa de identificação nacional e as duas biometrias em conjunto reduz ainda mais o número de possíveis excluídos.

Ademais, a íris pode ser coletada desde o nascimento, pois já está formada mesmo que a cor dos olhos ainda se altere. Inclusive mesmo pessoas com cegueira apresentam qualidade e possibilidade para a coleta da íris. Já no caso da impressão digital sabe-se que os sulcos papilares se distanciam até os sete anos de idade, exigindo, portanto, novas coletas após essa fase.

Destaca-se, por fim, que para a coleta da íris não é necessário contato entre o coletor e o requerente, o que no caso da impressão digital é inevitável.

Embora a falsificação e fraude de uma das duas biometrias supracitadas seja possível, ou seja, fraudar a íris ou a impressão digital, executar a mesma ação para as duas biometrias simultaneamente exigiria um esforço e habilidade tão superiores e complexos que inviabilizaria tais ataques maliciosos.

Aproveita-se a oportunidade para esclarecer que as demais biometrias estudadas (assinatura, face, veias da mão e voz) não apresentam ainda sistemas automatizados para busca **1: n** confiáveis e, portanto, não devem ser utilizados num programa de grande escala que preze pela qualidade da informação. Além disso, tais biometrias apresentam elevadas taxas de erros associados a vários outros critérios avaliados.

Assim, os signatários recomendam a utilização das biometrias íris e impressão digital para o Programa de Identidade Civil Brasileiro (RIC).

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.108/125
--------------------	---------------------	---	-------------

Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

ANEXO I – MAPAS MENTAIS

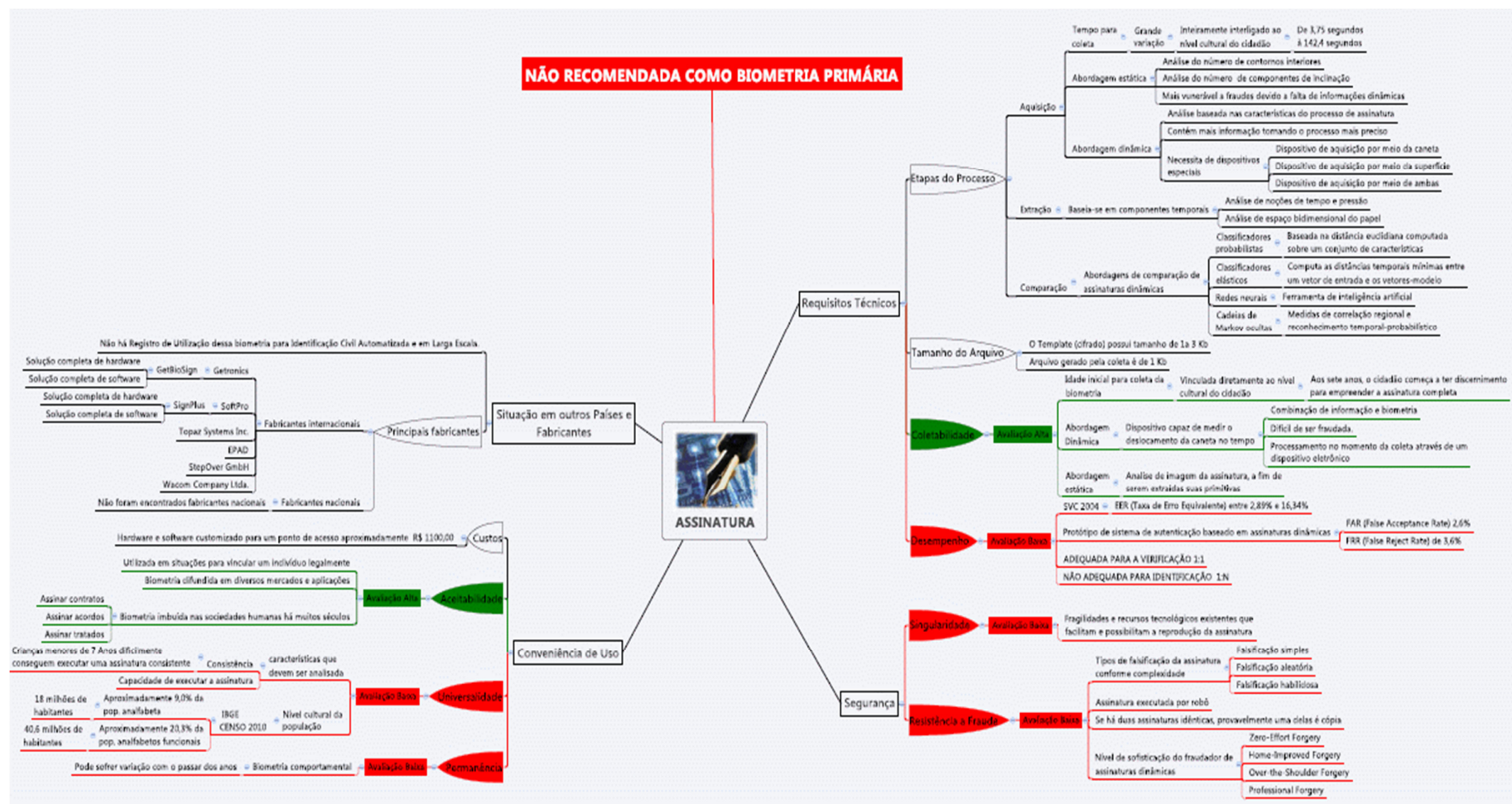
A apresentação dos mapas mentais das biometrias estudadas tem o objetivo de facilitar a avaliação da adequabilidade de aplicação da referida biometria para o Programa Brasileiro RIC considerando todos os aspectos acima referidos através da utilização visual de cores, sendo a cor verde uma avaliação positiva, cor amarela valoração média e cor vermelha como avaliação baixa. Critérios não coloridos foram descritos com objetivo de auxiliar o entendimento do mapa mental.

Projeto: MJ/SE-RIC	Emissão: 10/06/2014	Arquivo: 20140610 MJ RIC - RT das 6 (seis) Biometrias Provaveis de Utilizacao no RIC.docx	Pág.109/125
--------------------	---------------------	---	-------------

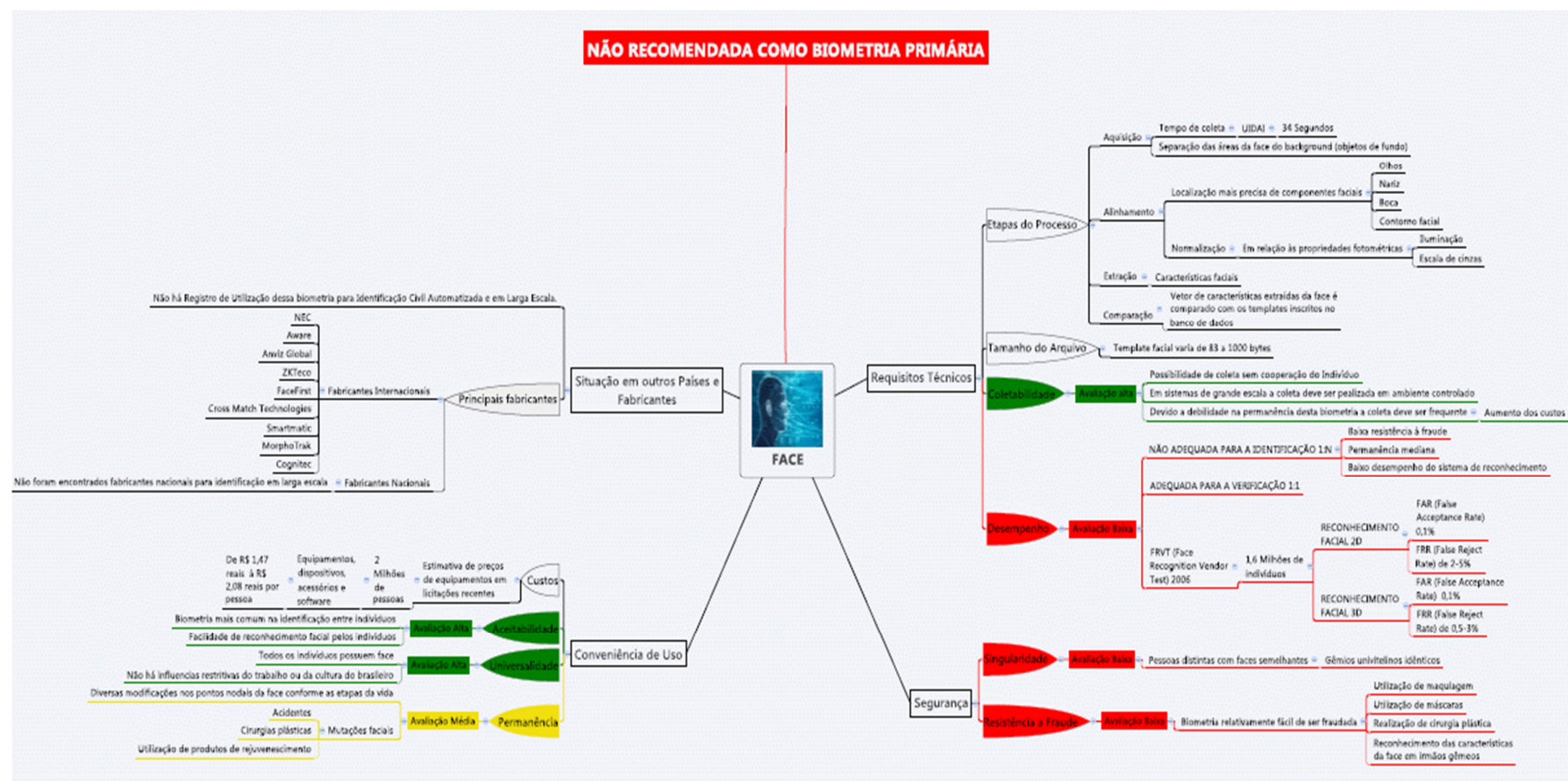
Confidencial.

Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

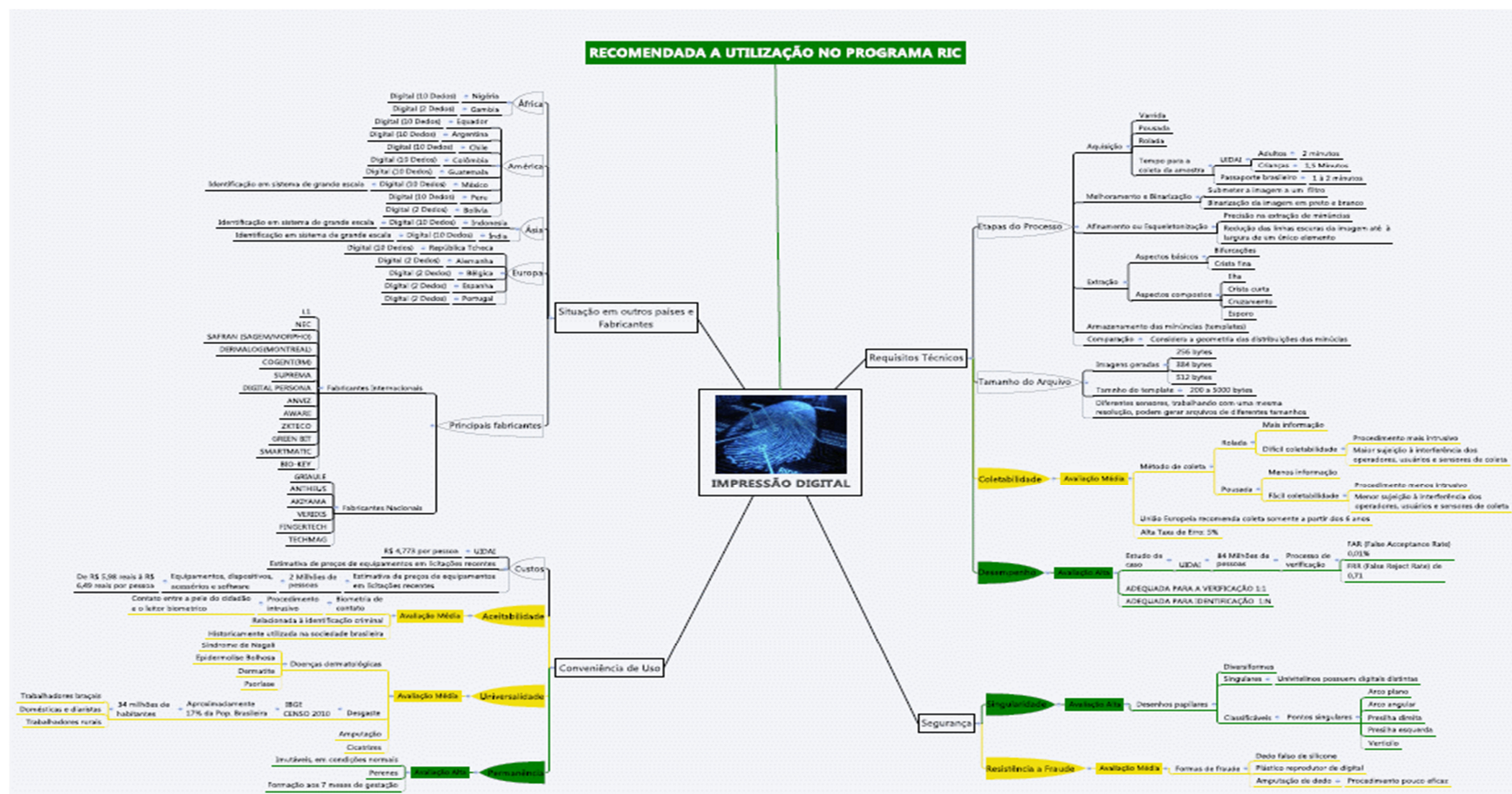
Mapa Mental Assinatura



Mapa Mental Face



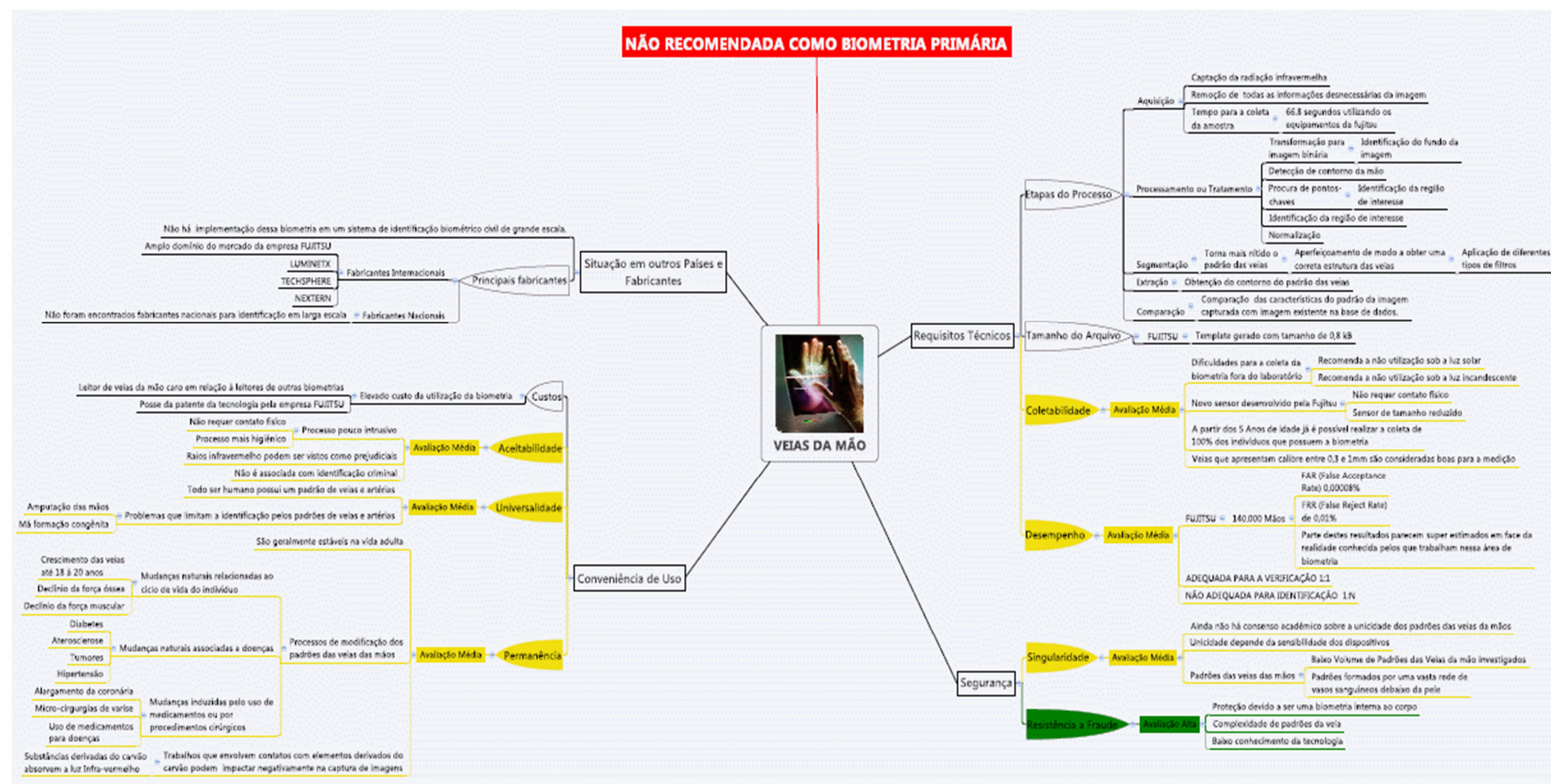
Mapa Mental Impressão Digital



Mapa Mental Iris



Mapa Mental Veias da Mão



Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

REFERÊNCIAS BIBLIOGRÁFICAS

(Aboalsamh, 2010)	ABOALSAMH, HATIM A. Vein and Fingerprint Biometrics Authentication-Future Trends. International Journal Of Computers And Communications, Accepted Oct, v. 5, 2010.
(ANP e INI, 2009)	ANP (Academia Nacional de Polícia) e INI (Instituto Nacional de Identificação), Departamento de Polícia Federal). Manual Cadastramento biométrico do eleitor brasileiro. Brasília, 2009.
(Azevedo et al, 2009)	Azevedo, Luciana Lemos de, et al. "Queixas vocais e grau de disfonia em professoras do ensino fundamental; Vocal complaints and degree of dysphonia in elementary school teachers." Rev. soc. bras. fonoaudiol 14.2 (2009): 192-196.
(Azevedo, 2011)	AZEVEDO, Augusto César Gonçalves de. Implementação de um método para Reconhecimento On-line de Assinaturas. 2011.
(Buiati, 2014)	Buiati, F., Panorama Geral das Biometrias, 2014.
(Camp, 2007)	CAMP, L. Jean. Economics of identity theft: Avoidance, causes and possible cures. Springer, 2007.
(Carreira, 2009)	CARREIRA, Ricardo Pereira de Oliveira. Concepção de um sistema alternativo de reconhecimento de Íris cooperativo. 2009. Tese de Doutorado. Master's thesis, Universidade da Beira Interior.
(Cavalcante et al, 2005)	CAVALCANTE, Adalberto Luiz Sobral; BACCI, Márcio Demétrio; HOKAMA, Marçal de Lima, Assinatura de Documentos Digitais através da Biometria no Exército Brasileiro, 2005
(Censo IBGE, 2010)	IBGE, Censo Demográfico. "Características gerais da população, religião e pessoas com deficiência." Instituto Brasileiro de Geografia e Estatística, Rio de Janeiro (2010).

(Champod et al, 2005)	CHAMPOD, Damien Dessimoz Jonas Richiardi Christophe; DRYGAJLO, Dr Andrzej. Multimodal Biometrics for Identity Documents State-of-the-Art. Research Report PFS 341-08.05 sept 2005.
(Costa et al, 2006)	COSTA, Luciano R.; OBELHEIRO, Rafael R.; FRAGA, Joni S. Introdução à Biometria. Livro texto dos Minicursos do VI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg2006). SBC: Porto Alegre, v. 1, p. 103-151, 2006.
(Costa, 2001)	COSTA, Silvia Maria Farani. Classificação e verificação de impressões digitais. Dissertação de Mestrado. Universidade de São Paulo, 2001.
(Daugman, 1994)	DAUGMAN, John G. Biometric personal identification system based on iris analysis. U.S. Patent n. 5,291,560, 1 mar. 1994.
(Daugman, 1999)	DAUGMAN, John, 1999. Recognizing Persons by their Iris Patterns. In Jain, A. K., Bolle, R., and Pankanti, S., editors, Biometrics: Personal Identification in Networked Society, pages 103- 122,. Kluwer Academic Publishers, London, UK.
(Daugman, 2004)	DAUGMAN, John. How iris recognition works. Circuits and Systems for Video Technology, IEEE Transactions on, v. 14, n. 1, p. 21-30, 2004.
(Decann, 2013)	DECANN, Brian; ROSS, Arun. De-duplication errors in a biometric system: An investigative study. In: Information Forensics and Security (WIFS), 2013 IEEE International Workshop on. IEEE, 2013. p. 43-48.
(Delgado, 2013)	DELGADO, Edmundo Daniel Hoyle. Reconhecimento Biométrico usando informação da Iris e de Características Perioculars. Tese de Doutorado. UFRJ, 2013.
(Dessimoz et al, 2007)	DESSIMOZ, Damien et al. Multimodal biometrics for identity documents. Forensic science international, v. 167, n. 2, p. 154-159, 2007.

(Edgington, 2007)	EDGINGTON, Ben. Your quest for the ideal biometric: is it in vain? Introducing Hitachi's, 2007.
(Faundez-Zanuy 2007)	FAUNDEZ-ZANUY, Marcos. On-line signature recognition based on VQ-DTW. Pattern Recognition, v. 40, n. 3, p. 981-992, 2007
(Figueiredo, 1994)	Figueiredo, Ricardo Molina de. "Identificação de falantes: aspectos teóricos e metodológicos", Unicamp, 1994.
(FpVTE 2003)	FpVTE 2003 - Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. US Department of Commerce, National Institute of Standards and Technology, 2004.
(Gafurov et al, 2010)	GAFUROV, Davrondzhon et al. Independent Performance Evaluation of Biometric Systems, 2010.
(Gelb e Clark, 2013)	GELB, Alan; CLARK, Julia. Performance Lessons from India's Universal Identification Program. 2013.
(Geradts e Sommer, 2006)	GERADTS, Zeno; SOMMER, P. Forensic implications of identity management systems. FIDIS WP6 Deliverable, v. 6, 2006.
(Grother et al, 2010)	GROTHER, Patrick J.; QUINN, George W.; PHILLIPS, P. Jonathon. Report on the evaluation of 2D still-image face recognition algorithms. NIST Interagency Rep, n. 7709, 2010.
(Guenter, 2013)	GUENTER, SCHUMACHER. Fingerprint Recognition for Children. JRC Technical Reports, EUR 26 193 EN, 2013.
(Guru et al, 2011)	GURU, D. S. et al. An Approach for Hand Vein Representation and Indexing. International Journal of Digital Crime and Forensics (IJDCF), v. 3, n. 2, p. 1-15, 2011.
(Hartung, 2012)	HARTUNG, Daniel. Vascular Pattern Recognition: And its Application in Privacy-Preserving Biometric Online-Banking Systems. 2012.

(Hawthorne, 2009)	HAWTHORNE, Mark. Fingerprints: analysis and understanding. CRC Press, 2009.
(Hedge et al, 2009)	HEGDE, Chetana et al. Authentication of damaged hand vein patterns by modularization. In: TENCON 2009-2009 IEEE Region 10 Conference. IEEE, 2009. p. 1-6.
(Heinen e Osorio, 2004)	HEINEN, Milton Roberto; OSÓRIO, Fernando Santos; EXATAS, Ciências. Biometria comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas. Infocomp Revista de Ciência da Computação, 2004.
(Hong et al, 2005)	HONG, Jin-Hyuk; YUN, Eun-Kyung; CHO, Sung-Bae. A review of performance evaluation for biometrics systems. International Journal of Image and Graphics, v. 5, n. 03, p. 501-536, 2005.
(IBG, 2005)	IBG - International Biometric Group. Independent Testing of Iris Recognition Technology. Final Report, 2005
(Jain e Kumar, 2010)	JAIN, Anil K.; KUMAR, Ajay. Biometrics of next generation: An overview. Second Generation Biometrics, 2010.
(Jain e Li, 2005)	JAIN, Anil K.; LI, Stan Z. Handbook of face recognition. New York: springer, 2005.
(Jain e Pankanti, 2008)	JAIN, Anil K.; PANKANTI, Sharath. Beyond fingerprinting. Scientific American, v. 299, n. 3, p. 78-81, 2008.
(Jain et al, 2002)	JAIN, Anil K.; GRIESS, Friederike D.; CONNELL, Scott D. On-line signature verification. Pattern recognition, v. 35, n. 12, p. 2963-2972, 2002.
(Jain et al, 2004)	JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil. An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions on, v. 14, n. 1, p. 4-20, 2004.
(Jain et al, 2007)	JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. Handbook of biometrics. Springer, 2007.

(Justino, 2001)	JUSTINO, E. O Grafismo e os Modelos Escondidos de Markov na Verificação Automática de Assinaturas. Tese de Doutorado, Pontifícia Universidade Católica do Paraná, Brasil, 2001
(Karnopp, 2004)	Karnopp, Lodenir Becker. "Aquisição da linguagem por crianças surdas—investigações sobre o léxico." <i>Calidoscópio</i> 2.1 (2004): 75-88.
(Klokova, 2010)	Alina Klokova, "Comparison of Various Biometric Methods", Interactive Multimedia Systems, Electronics and Computer Science, University of Southampton, 2010. Link: http://mms.ecs.soton.ac.uk/2011/papers/4.pdf .
(Kumar e Prathyusha, 2009)	KUMAR, Ajay; PRATHYUSHA, K. Venkata. Personal authentication using hand vein triangulation and knuckle shape. Image Processing, IEEE Transactions on, v. 18, n. 9, p. 2127-2136, 2009.
(Li e Jain, 2009)	LI, Stan Z.; JAIN, Anil Kumar. Encyclopedia of Biometrics: I-Z. Springer, 2009.
(Mali e Bhattacharya, 2013)	MALI, Kalyani; BHATTACHARYA, Samayita. Comparative Study of Different Biometric. International Journal Of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.
(Maltoni et al, 2009)	MALTONI, Davide et al. Handbook of fingerprint recognition. Springer, 2009.
(Modi, 2011)	MODI, Shimon K. Biometrics in Identity Management: Concepts to Applications. Artech House, 2011.
(Moraes, 2006)	DE MORAES, ALEXANDRE FERNANDES. "Método para avaliação da tecnologia biométrica na segurança de aeroportos." (2006).
(Murari, 2013)	MURARI, Juliano Ferreira Jorge. Detecção de vivacidade em sistemas de reconhecimento de íris. Mestrado Integrado em Engenharia Eletrotécnica e de Computadores. FEUP - Universidade do Porto. 2013.

(Muroò et al, 2000)	MUROÒ, Ale and POSPISIL Jaroslav et al. The human iris structure and its usages. Acta Univ. Palacki. Olomuc., 39:87-95, March 2000.
(Myers e Rabiner, 1981)	MYERS, Cory S.; RABINER, Lawrence R. A Comparative Study of Several Dynamic Time-Warping Algorithms for Connected-Word Recognition. Bell System Technical Journal, v. 60, n. 7, p. 1389-1409, 1981
(Nadort, 2007)	NADORT, Annemarie. The hand vein pattern used as a biometric feature. Master Literature Thesis of Medical Natural Sciences at the Free University, Amsterdam, 2007.
(Nandakumar et al, 2010)	NANDAKUMAR, Karthik et al. Anil K. Jain, Michigan State University Jianjiang Feng, Tsinghua University, Beijing. 2010. Fingerprint Matching - IEEE Computer – pg. 36-44. 2010.
(Negin et al, 2000)	NEGIN, Michael et al. An iris biometric system for public and personal use. Computer, v. 33, n. 2, p. 70-75, 2000.
(Olatinwo et al, 2013)	OLATINWO, Segun O.; SHOEWU, O.; OMITOLA, Olusegun O. Iris Recognition Technology: Implementation, Application, and Security Consideration. The Pacific Journal of Science and Technology, Volume 14. Number 2. November 2013.
(Padovani e Teixeira, 2005)	PADOVANI, Carla Marcondes César Affonso; TEIXEIRA, Elizabeth Reis. Do balbucio à fala–reflexões sobre a importância das atividades lingüísticas iniciais eo desenvolvimento da linguagem oral em crianças com deficiência auditiva. Distúrbios da Comunicação. ISSN 2176-2724, v. 17, n. 1, 2005.
(Petitimbert et al, 2011)	PETITIMBERT, C; DISTLER, M; MYRTUE, N. G.; JENSEN, S. N. Biometric Identification using Hand Vein Patterns, 2011.
(Phillips et al, 2003)	PHILLIPS, P. Jonathon et al. Face recognition vendor test 2002. In: Analysis and Modeling of Faces and Gestures,

	2003. AMFG 2003. IEEE International Workshop on. IEEE, 2003. p. 44.
(Rabiner e Juang, 1986)	Rabiner, L. R. and Juang, B. H. (1986). An introduction to Hidden Markov Models. IEEE Magazine on Accoustics, Speech and Signal Processing, 3(1):4-16.
(Rasha, 1994)	RASHA, ABAS. A Prototype System for Off-Line Signature Verification Using Multilayered Feedforward Neural Networks. Master's Thesis, RMIT Department of Computer Science, Melbourne, 1994.
(Revett, 2008)	REVETT, Kenneth. Behavioral biometrics. New York, NY: John Wiley e Sons. doi, v. 10, p. 9780470997949, 2008.
(Ross et al, 2006)	ROSS, Arun A.; NANDAKUMAR, Karthik; JAIN, Anil K. Handbook of multibiometrics. Springer, 2006.
(Sá et al, 2012)	Sá, Angela Abreu Rosa de, et al. "Interface computacional de biometria como ferramenta de apoio à perícia de confronto de voz" Rev. Bras. Biom., São Paulo, v. 30, n.4, p.442 – 460, 2012
(Sabourn e Genest, 1994)	SABOURIN, R.; GENEST, G. An Extended-Shadow-Code Based Approach for Off-Line Signature Verification. 12th IAPR International Conference on Pattern Recognition, Israel, 1994, 450-460 p.
(Santos, 2004)	SANTOS, CESAR ROBERTO. Análise de assinaturas manuscritas baseada nos princípios da grafoscopia. 2004. Tese de Doutorado. Master's thesis, Pontifícia Universidade Católica do Paraná.
(UIDAI 2009)	Udai, Committee on Biometrics - Biometrics Design Standards For UID Applications. 2009.
(UIDAI 2012a)	Udai, Role of Biometric Technology in Aadhaar Authentication. Authentication Accuracy Report: Unique Identification Authority of India. 2012.
(UIDAI 2012b)	Udai, Role of Biometric Technology in Aadhaar Authentication: IRIS Authentication Accuracy – PoC Report: Unique Identification Authority of India. 2012.

(UIDAI 2012c)	Uidai, Role of Biometric Technology in Aadhaar Enrollment: Unique Identification Authority of India. 2012.
(UIDAI 2012d)	Uidai, Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission. 2012.
(Vieira et al, 2010)	VIEIRA, Danielle Caled; Silva, Davi Mattos de Carvalho Sanches; Barbosa, Robert Ribeiro; Carvalho, Rodrigo Pinheiro; Biometria – Assinatura, 2010.
(Vigliazi, 2006)	VIGLIAZZI, Douglas. Biometria-Medidas de Segurança. Rio de Janeiro, v. 2, 2006. LIVRO
(Wang e Leedham, 2005)	WANG, Lingyu; LEEDHAM, Graham. A thermal hand vein pattern verification system. In: Pattern Recognition and Image Analysis. Springer Berlin Heidelberg, 2005. p. 58-65.
(Wilson, 2011)	WILSON, Chuck. Vein pattern recognition: a privacy enhancing biometric. CRC press, 2011.
(Xueyan e Shuxu, 2008)	XUEYAN, Li; SHUXU, Guo. The Fourth Biometric-Vein Recognition. Pattern Recognition Techniques, Technology and Applications, v. 626, 2008.
(Yabu-uti, 2004)	YABU-UTI, João Batista Tadanobu. Sistemas Computadorizados para Reconhecimento de Pessoas. Revista On- Line, Instituto de Engenharia Biomédica UFSC, abr. 2004.
(Yeung et al, 2004)	YEUNG, Dit-Yan et al. SVC2004: First international signature verification competition. In: Biometric Authentication. Springer Berlin Heidelberg, 2004. p. 16-22.
(Yuksel et al, 2010)	YUKSEL, A.; AKARUN, Lale; SANKUR, Bülent. Biometric identification through hand vein patterns. In: Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB), 2010 International Workshop on. IEEE, 2010. p. 1-6.
(Zhu et al, 2000)	ZHU, Yong; TAN, Tieniu; WANG, Yunhong. Biometric personal identification based on iris patterns. In: Pattern

	Recognition, International Conference on. IEEE Computer Society, 2000. p. 2801-2801.
--	--

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br

