Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação

Uma Proposta para Melhoria na Eficiência de um Sistema de Reconhecimento de Íris Humana.

Autor: Roger Fredy Larico Chavez
Orientador: Prof. Dr. Yuzo Iano

Dissertação de Mestrado apresentada à Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: **Telemática e Telecomunicações**.

Banca Examinadora

Yuzo Iano	Decom/Feec/Unicamp
Osamu Saotome	IEEA/IEE/ITA
André Leon Sampaio Gradvohl	Cenapad/Unicamp
João Baptista Tadanobu Yabu-uti	Decom/Feec/Unicamp

Campinas, SP
Fevereiro/2007

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

L324p

Larico Chavez, Roger Fredy
Uma proposta para melhoria na eficiência de um sistema de reconhecimento de íris humana / Roger Fredy Larico Chavez. --Campinas, SP: [s.n.], 2007.

Orientador: Yuzo Iano
Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Íris (Olhos). 2. Reconhecimento de padrões. 3. Biometria. 4. Processamento de sinais. 5. Processamento de imagens. 6. Computação – Medidas de segurança. I. Iano, Yuzo. II. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. III. Título.

Título em Inglês: A new proposal for improvement in the iris recognition system
Palavras-chave em Inglês: Iris recognition, biometric, security, Algorithms, Acquire, segmentation, detection of circles, Signal processing
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Osamu Saotome, André Leon Sampaio Gradvohl e João Baptista Tadanobu Yabu-uti
Data da defesa: 28/02/2007
Programa de Pós-Graduação: Engenharia Elétrica

Resumo

A biometria tem sido utilizada amplamente em segurança de sistemas automatizados. Neste trabalho propõe-se um sistema de reconhecimento pessoal baseado na biometria de íris. Essa escolha baseia-se no fato de que a íris fornece uma das melhores formas de biometria, atualmente. Tem-se como objetivo, estudar e melhorar os métodos existentes visando uma diminuição no tempo de processamento, na quantidade de memória requerida bem como na porcentagem de erros. A pesquisa mostra que o bloco mais lento corresponde ao da localização. O bloco que insere mais erros no processo de reconhecimento é o da captura de dados, isso porque a coleta de informações é feita por um dispositivo (câmera) em um ambiente onde muitos fatores transformam-se em fontes de erros. Os algoritmos de reconhecimento estudados visam uma percentagem de erro mínimo.

Para o desenvolvimento de um algoritmo rápido visando o reconhecimento de íris, é necessária uma localização adequada da imagem, com pouca perda de informação. Neste trabalho, também se apresenta um algoritmo detalhado de localização rápida da textura da íris. Para isso, se utiliza um esquema de busca iterativa de centros e raios de círculos concêntricos bem como a aplicação de ruído gaussiano e a utilização de filtros medianos para se conseguir uma resposta confiável. Os resultados encontrados são comparados com algoritmos publicados na literatura e exaustivamente testados. O algoritmo proposto apresenta desempenho superior em comparação com outros em relação à velocidade de processamento assim como um incremento na exatidão de reconhecimento.

Palavras-chave: Reconhecimento de íris, biometria, segurança, algoritmos, captura, localização, detecção de círculos, processamento de sinais.

Abstract

The biometric has been widely used in automated security systems. In this work we propose a biometrics personal identification system based on iris, due to its better biometrics parameters results. The purpose of this study is to improve existing methods aiming to decrease the processing time, the required storage memory and the error rate. Our research shows that the slowest operation is the segmentation of iris. Also, the block that adds more errors in the recognition process is the data capture, due to the fact it is made by a device (camera) in such environment that many factors can become source of errors. The studied recognition algorithms search for a minimum error percentage.

In order to develop a fast algorithm for iris recognition we need a fine segmentation image, with a low loss of information. In this work, we also present a detailed algorithm for the fast segmentation of iris texture that was achieved using an iterative search for centers and radius of concentric circles, as well as the application of Gaussian noise and the utilization of median filters to get reliable results. The achieved results are evaluated and compared to the published algorithms. The algorithm presents a better performance with relation to processing speed as well as an improvement of the recognition precision.

Keywords: Iris Recognition, biometric, security, algorithms, acquire, segmentation, detection of circles, signal processing.

A Deus pelo caminho que marcou para mim.

Agradecimentos

Ao meu orientador, Prof. Yuzo Iano sou grato pela orientação, conselhos e compreensão.

Agradecimento especial para o Prof. Vicente Idalberto Becerra Sablón, que acompanhou de modo atuante o presente trabalho desde o início de minha pesquisa.

Aos demais colegas de pós-graduação, pelas sugestões, conselhos e amizade.

A minha família e meus amigos pelo apoio durante esta jornada.

Agradeço ao pesquisador J. G. Daugman que forneceu os elementos de base teórica para esta pesquisa. Também ao pesquisador L. Masek que proveu os subsídios para o desenvolvimento em Matlab (ponto de partida para substituições e comparações). Agradeço muitíssimo a Academia Chinesa de Ciências - Instituto de Automação (CASIA - *Chinese Academy of Sciences - Institute of Automation*) pelo banco de dados contendo as imagens de íris que foram utilizadas neste trabalho.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

I(x, y)	*Image,* imagem digital matricial.
$\boldsymbol{Z_i f}$	*Zero crossing,* no nível *i* da função *f*.
$\psi_{a,b}$	Funções *wavelets*.
MaskN	Matriz máscara corresponde a imagem N.
Δt	Variação de tempo.
(X_m, Y_m)	Coordenadas cartesianas em uma imagem, para *m*: p (pupila), i (íris).
R_m, R_m^e	Raios *m*: p (pupila), i (íris), *e:* eixo x ou y.
G_σ	Função gaussiana.

Abreviaturas

CMOS – *Complementary Metal Oxide Semiconductor,* Semicondutor Metal Óxido complementar.

EER – *Equal Error Rate*, Taxa de Erro Igual.

FAR – *False Acceptation Rate*, Taxa de Falsa Aceitação.

FDPA – Função de Distribuição de Probabilidade Acumulada

FRR – *False Rejection Rate*, Taxa de Falsa Rejeição.

HD – *Hamming Distance*, Distância de Hamming.

ICA – *Independent Component Analysis*, Análise Independente de Componentes.

M-ICA – *Multiresolution Independent Component Analysis*, Análise ICA em várias Resoluções.

OFDM – *Orthogonal Frequency Division Multiplexing,* Multiplexagem por Divisão de Freqüência Ortogonal.

PIN – *Personal Identification Number*, Código de Identificação Pessoal.

RDBMS – *Relational Database Management System*, Sistema de Gerenciamento de Base de Dados.

ROC – *Receiver Operating Characteristi*c, Característica de Operação de Recepção.

ROI – *Return Of Invest*, Retorno de Investimento.

ROI* – *Region Of Interest*, Região de Interesse.

SDK – *Software Developed Kit,* Conjunto de Aplicações para Suporte de Alguma Aplicação.

TH – Transformada de Hough.

TWC – Transformada de *Wavelets* Contínua.

TWD – Transformada de *Wavelets* Discreta.

XOR – Exclusive OR, Operação Booleana OU Exclusivo.

ZeroFAR – Ponto onde o FAR converge a zero.

ZeroFRR – Ponto onde o FRR converge a zero.

Publicações

1. Roger F. Larico, Y. Iano, V. Sablón. “Processo de Reconhecimento de Íris Humana: Localização Rápida de Íris”. Telecomunicações, Inatel, Nov. 2006.
2. Roger F. Larico Chavez, Y. Iano, V. Sablón. “Localização Rápida da Íris do Olho Humano”. Rev. Ciência e Tecnologia Unisal. São Paulo, SP, 2007.
3. Roger F. Larico, Yuzo Iano, Vicente B. Sablon; “Sistema Eficiente de Reconhecimento de Íris Humana: Localização”, XIII Congreso Internacional de Ingenieria Electronica, Electrica y de Sistemas. Universidad Nacional del Callao. Callao, Perú. Ago. 2006.
4. Roger F. Larico, Yuzo Iano, Vicente B. Sablón; "Sistema Eficiente de Reconhecimento de Íris Humana", I Encontro de Ciência e Tecnologia dos Estudantes Latino-Americanos da Unicamp, Universidade Estadual de Campinas. São Paulo, Brasil. Nov. 2005.
5. Rangel Arthur, Y. Iano, S. Carvalho, Roger F. Larico Chavez. “Planificación de la Expansión del Servicio de Retransmisión de TV Digital en Brasil usando redes SFN”. Revista IEEE América Latina. IEEE Región 9. 2006. (Aceito)
6. Roger F. Larico, Yuzo Iano, Vicente B. Sablón, “Processo de Reconhecimento de Íris Humana: Localização Rápida de Íris,“5th Latin American and Caribbean Conference for Engineering and Technology, 2007 (aceito)
7. Víctor H. Alvarez, Roger F. Larico, Yuzo Iano, Martín Aznar, Parameter Estimation for VLE Calculations by Global Minimization through Genetic Algorithm”. Brazilian Journal of Chemical Engineering, 2007.
8. Roger F. Larico. “Process of Recognition of Human Iris: Fast Segmentation of the Iris”. IEEE Transactions on Pattern Analysis and Machine Intelligence. TPAMI-0785-1106, 2006. (submetido)

Capítulo 1

Introdução

Um dos grandes problemas encontrados em países, bem como em indústrias e organizações de maneira geral, é a garantia de se prover sistemas de identificação pessoal que ofereçam serviços seguros e confiáveis. Essa preocupação vai desde evitar fraudes e falsificações de documentos até prevenir roubos de dados e segredos industriais. Esse quadro tem motivado muitas pesquisas sobre sistemas de identificação pessoal baseados em características biométricas.

A biometria apresenta vantagens em relação aos meios convencionais de identificação, tais como cartões de identidade ou senhas, pois permite a utilização de características intrínsecas às pessoas. Conseqüentemente, ela dificulta a falsificação e o roubo porque envolve o histórico biométrico de uma pessoa que, em geral, tende a permanecer estável na fase adulta. Em virtude dessa vantagem cresce o número de aplicações de sistemas biométricos tanto no Brasil quanto em todo o mundo [w1].

Dentro desse contexto, a íris humana apresenta um conjunto de propriedades que a qualifica como um dos sistemas mais seguros de reconhecimento biométrico. De fato, entre todas as biometrias, a íris se apresenta como sendo uma das mais confiáveis e com taxas mínimas de erro de reconhecimento.

Como em todas as áreas do conhecimento, hoje há uma farta literatura disponível que descreve os principais métodos de reconhecimento de íris propostos. Porém, ela se apresenta ainda de forma fragmentada e incompleta, talvez devido aos interesses financeiros envolvidos uma vez que há uma tendência de se preservar segredos de tecnologia com potencial comercial. Entre os algoritmos de reconhecimento de íris descritos na literatura [1], o algoritmo de J. Daugman tem os melhores resultados.

Áreas de concentração

Este trabalho aborda basicamente duas áreas de conhecimento:

- **Processamento digital de sinais e de imagens**: isso devido à necessidade de se gerar métodos que possibilitem a criação de um vetor característico correspondente a uma imagem de um olho aplicando-se uma segmentação, bem como uma normalização.
- **Reconhecimento de padrões**: isso porque se necessita de métodos para classificação de elementos num conjunto de dados, com base em características associadas a tais elementos selecionados.

As máquinas podem observar um meio, aprender a distinguir padrões de interesse nesse meio e ser capazes de tomar decisões corretas sobre as categorias a que pertencem tais padrões [2]. No estudo da biometria, que é uma das aplicações de reconhecimento de padrões, escolheu-se neste trabalho o padrão correspondente à textura de íris pelas razões já comentadas.

1.1 História

Aparentemente, foram os parisienses os primeiros a utilizar o reconhecimento de íris como base para a identificação de pessoas. Um oficial da polícia francesa, não satisfeito com a forma de se identificar os criminosos reincidentes, apresentou em 1882 uma técnica de identificação baseada em medição de alguma característica de corpo humano. Passaram então a distinguir os condenados de seu sistema penal, inspecionando visualmente suas íris, tendo como base a sua cor [3]. Mais recentemente, o conceito de reconhecimento automático de íris foi proposto por Flom e Safir [4], porém esse grupo não chegou a desenvolver e testar um sistema. Trabalhos mais recentes com o objetivo de se construir um sistema de reconhecimento automático baseado em íris foram conduzidos em *Los Alamos National Laboratories, CA* [5].

Em seguida, dois grupos de pesquisa liderados por J. Daugman e R. Wildes, desenvolveram e documentaram um protótipo de um sistema biométrico utilizando a íris como uma característica básica [2], [6]. Outras pesquisas foram sendo desenvolvidas por W. Boles em 1998, Shinyong Lim em 2001, T. Yong Zhu em 2000, Seung-In Noh em 2002 e C. Tisse em 2003 [68], [75], [74].

1.2 Problema

A necessidade de se controlar o acesso a áreas restritas, torna-se cada vez mais importante atualmente. O procedimento comumente usado é a confirmação de uma senha ou *password* pessoal. Mas esse mecanismo, embora seja muito prático, é ainda frágil devido ao fato de que os usuários às vezes utilizam senhas simples ou chegam até mesmo a esquecê-las. Outro método é o uso de cartão que apresenta os inconvenientes de extravio, roubo e clonagem. Técnicas biométricas atuais, onde as características usadas dificilmente podem ser roubadas ou duplicadas, ainda não têm a importância adequada em nosso meio, justificando assim, mais pesquisas que possam ter aplicações práticas.

A biometria pode ser utilizada para o processo de autenticação, mas existe uma variedade grande de tecnologias biométricas, sendo que cada uma delas utiliza características biométricas que procuram aumentar o grau de confiança dos usuários em relação à segurança do sistema. A implantação de um sistema biométrico tem ainda um custo alto e depende da técnica biométrica adotada. Mas, a escolha de um sistema biométrico influi diretamente no grau de segurança e no custo de implantação e manutenção, ou seja, tem implicações financeiras a curto e longo prazo. Na verdade, sente-se falta de critérios apropriados para a escolha adequada de uma biometria, levando-se em conta também, a facilidade de uso.

No caso específico da biometria baseada em íris, as publicações apresentam um claro padrão em que o processo de reconhecimento tradicional é lento. Portanto, isso dificulta a aplicação desses procedimentos em um sistema computacional em tempo real. Além disso, a utilização de quantidade de memória é alta, por exemplo, na detecção de circunferências de íris e pupila seja por meio de transformadas ou por métodos integro-diferenciais, tornando o processo todo altamente dispendioso em termos de memória. Também o custo relacionado à aquisição de dados é caro sendo essencial uma análise e uma escolha de um bom dispositivo de captura. Essa etapa pode ser muito difícil de concluir em definitivo devido ao fato de que as variáveis a serem levadas em conta envolvem aspectos tanto objetivos quanto subjetivos (ex: custo, luminância, resolução, definição da lente, iluminação, ambiente, resposta em freqüência, câmera, etc).

1.3 Objetivos

Os objetivos desta dissertação estão voltados principalmente para melhorias de um sistema de identificação biométrica baseada em íris, a fim de torná-lo mais eficiente. De acordo com publicações técnicas na Europa [8], [9] e organismos internacionais [10], sistemas biométricos baseados em íris são promissores em relação à utilização prática. Neste trabalho, apresentam-se também considerações para uma escolha adequada de características biométricas e assim justificar um pouco mais a escolha de íris como tema desta pesquisa. Dessa forma, são enfocados os seguintes itens:

- Definição e seleção adequada de sistemas biométricos, com enfoque em sistemas que utilizam medida de íris.
- Propostas de melhorias de um sistema biométrico baseado em reconhecimento de íris.
- Em um sistema biométrico proposto, tornar o processo de reconhecimento mais rápido do que os da literatura atual. Isso sem diminuir a exatidão nem aumentar os recursos disponíveis. Para tanto, foi necessário:
    - Estudar a estrutura de um sistema de reconhecimento de íris, no contexto da biometria e de sistemas biométricos.
    - Identificar a parte ou bloco que insere mais erros no processo.
    - Identificar os blocos mais lentos do processo e melhorar ou substituir o algoritmo associado.

1.4 Considerações Iniciais

Grande parte das simulações foi baseada no sistema de J. Daugman [2] implementado por L. Masek [11], [12]. Dessa forma, pôde-se comparar com o mesmo, o desempenho do sistema melhorado proposto. Em todas as etapas foram utilizadas as técnicas sugeridas nesse trabalho de referência, sendo que a única variação entre os dois sistemas acontece na etapa de localização.

Para a simulação e avaliação do sistema, foram utilizadas as imagens de íris do banco de imagens da Academia Chinesa de Ciências - Instituto de Automação (CASIA - *Chinese Academy of Sciences - Institute of Automation*) [13].

Os resultados para avaliação de eficiência baseiam-se em medidas de tempo de processamento. Além disso, preserva-se praticamente a mesma taxa de erro, e usa-se a mesma quantidade de memória no máximo.

1.5 Estrutura da Dissertação

Todas as informações envolvidas no desenvolvimento desta dissertação estão descritas em cada um dos capítulos que compõe a presente pesquisa.

- Capítulo 1: Introdução e apresentação dos objetivos e da estrutura da dissertação.
- Capítulo 2: Conceitos e definições básicas sobre biometria e informações técnicas biométricas utilizadas na pesquisa proposta.
- Capítulo 3: Formas e considerações para se escolher uma biometria, levando-se em conta a existência de vários métodos ou critérios propostos por diversas instituições.
- Capítulo 4: Nesse capítulo se apresentam algumas das mais conhecidas tecnologias biométricas aplicadas atualmente a fim de conhecê-las e compará-las.
- Capítulo 5: Aqui se apresenta amplamente uma tecnologia baseada em íris, apresentando-se as características da íris, alguns algoritmos comumente utilizados e aplicações.
- Capítulo 6: A maior parte da contribuição deste trabalho encontra-se neste capítulo, onde se detalha as melhorias do sistema de reconhecimento de íris proposto. Sobretudo, enfoca-se a implementação do bloco de localização que reduz muito, o tempo total do processamento. Apresentam-se também os resultados e as simulações efetuadas bem como uma comparação entre o algoritmo proposto e o clássico, envolvendo também comparações com resultados publicados na literatura atual.
- Capítulo 7: Apresentam-se conclusões finais e sugestões para trabalhos futuros.
- Na parte final da dissertação são anexados os apêndices, contendo informações adicionais, programas e figuras resultantes das simulações.

Capítulo 2

Conceitos Básicos de Biometria

Neste capítulo apresentam-se conceitos sobre biometria que foram utilizados durante a pesquisa. Tais conceitos são utilizados na área que trata de desenvolvimento de sistemas de identificação.

2.1 Biometria

Biometria (bio-metria: vida-medida) refere-se ao estudo estatístico das características físicas ou comportamentais dos seres vivos. Também se pode defini-la como sendo um ramo da ciência que estuda a mensuração dos seres vivos [14]. Essa palavra, à primeira vista, pode parecer nova, enquanto que para outros pode ser associada a alguma tecnologia futurística e complexa. No entanto, o conceito que ela encerra é bem mais simples e muito antigo, se refere ao reconhecimento de pessoas. Então a biometria trata da mensuração 'automática' de certas características físicas ou comportamentais de um determinado indivíduo bem como da comparação destas com a de outros tendo como objetivo a identificação ou o reconhecimento [15].

A biometria recentemente foi associada unicamente à medida de características físicas ou comportamentais de pessoas como forma de identificá-las. A premissa em que se fundamenta é a de que cada indivíduo é único e possui características físicas e de comportamento distintas (a voz, a maneira de andar, etc.).

A biometria pode ser utilizada para se identificar pessoas porque ela revela dados com certa exatidão, como um PIN (*Personal Identification Number*) ou senha. Mas a característica crucial que a torna diferente de outros métodos de identificação é que a biometria mede um parâmetro que é inerentemente própria de uma pessoa, individualizando-a [16].

As definições anteriores são independentes da medida biométrica, entretanto elas dão ênfase em características físicas ou comportamentais únicas e intransferíveis (ver Fig. 2.1)

[w2]. Assim, uma biometria baseia-se em uma característica distinguível entre pessoas diferentes (*'distinctive'*), sendo que essa característica varia dependendo da técnica usada para mensurá-lo [8].

Fig. 2.1 Características físicas e comportamentais utilizadas (únicas e distinguíveis [w2], [w3]).

Vantagens das características biométricas:

- Estão sempre disponíveis.
- São intransferíveis.
- São únicas para cada indivíduo.
- A variação entre os indivíduos é alta.

Em casos patológicos resultantes de muita pressão emocional ou de consumo de narcóticos, essas características não estão prontamente disponíveis. O estado emocional, em alguns tipos de biometria, afeta a característica em questão. Por exemplo, em biometria que leva em conta a maneira de digitação.

2.2 Tecnologias Biométricas

A biometria está relacionada diretamente com as **tecnologias biométricas** que são definidas como: métodos automáticos de verificação ou identificação de identidade de uma pessoa viva baseados em características fisiológicas ou de comportamento [17].

O sistema biométrico utiliza-se de características físicas (definidas como algo que se possui), e de características comportamentais (algo que se faz). Entre elas, destacam-se:

Características físicas:

- Composição química do odor corpóreo,

- Característica facial,
- Emissão de calor,
- Característica do olho (retina e íris),
- Impressão digital,
- Geometria da mão.

Características comportamentais:

- Assinatura,
- Dinâmica da digitação,
- Voz e forma de falar.

Dessas características, apenas três características físicas (a retina, a íris e a impressão digital) e todas as características comportamentais, usadas atualmente nos sistemas biométricos disponíveis, podem ser consideradas realmente únicas [15].

As definições de tecnologia biométrica contêm palavras chave como método automático e tipologia de autenticação. Estas são descritas a continuação [18].

2.2.1 Métodos Automáticos

Os componentes básicos para se implementar um sistema biométrico digital são:

- **Mecanismo de captura** de um sinal digital de uma característica pessoal.
- **Processamento e classificação** dos sinais capturados.
- **Interface homem e os dispositivos** que permitem ao usuário fazer a entrada de dados no sistema para que se realizem as tarefas de verificação e identificação automáticas.

O método é automático quando todos os processos envolvidos após a captura do sinal são feitos sem intervenção humana. Em geral, os métodos automáticos trabalham com as características de pessoas vivas.

A fim de se evitar fraudes, são inseridos detectores nos dispositivos de captura dos sistemas biométricos que determinam a existência de uma característica "viva", denominada *liveness* (Apêndice B.2).

Uma característica fisiológica é uma propriedade física relativamente estável tal como as impressões digitais, geometria da mão, padrão da íris, padrão dos vasos sangüíneos do fundo dos olhos, entre outras. Esse tipo de característica é basicamente imutável. Por outro lado, uma característica de comportamento é mais um reflexo de atitudes psicológicas do indivíduo. A assinatura é a característica de comportamento mais utilizada para autenticação. Outros comportamentos que podem ser utilizados são: a) forma como se digita nos teclados e b) maneira de se falar. As características de comportamento tendem a

variar com o tempo e por isso, muitos sistemas biométricos permitem que sejam feitas atualizações de seus dados biométricos de referência à medida que esses vão sendo utilizados [w4]. Em geral, ao se realizar a tarefa de atualização de dados, o sistema baseado em características de comportamento tende a ser mais eficiente em autenticar ou não o indivíduo. No entanto, esse recurso aumenta os custos de manutenção e operação.

A variação da característica fisiológica é menor do que em uma característica de comportamento. A estrutura da íris, em geral não muda ao longo da vida depois dos dois anos de idade. Uma assinatura, por outro lado, é influenciada tanto por fatores fisicamente controláveis quanto por fatores emocionais. Assim, sistemas baseados em comportamento necessitam de um grande esforço para se ajustar às variações intraclasse. Por isso, é mais fácil construir um sistema que, por exemplo, force o usuário a colocar a palma de sua mão sempre em uma determinada posição, do que implementar um algoritmo que reproduza o estado emocional de uma pessoa. No entanto, tanto as técnicas de comportamento quanto as fisiológicas resultam em sistemas de identificação de maior segurança do que aqueles baseados apenas em senhas e cartões.

2.2.2 Tipologia de Métodos de Autenticação

Em geral, a implementação de sistemas de identificação pessoal está baseada em chaves ou senhas, ou então em um dispositivo de autenticação utilizando características biométricas. Esses esquemas podem se mesclar, variando-se tanto a complexidade quanto a utilização de recursos a fim de se atender às exigências de um determinado projeto ou cliente. Os exemplos mais comuns de mistura são: os cartões magnéticos, senhas e digitais de dedos. As combinações mais comuns e práticas têm resultado no uso de cartão magnético juntamente com uma senha de conhecimento do usuário, cartão magnético juntamente com uma biometria de geometria de mão [w5], entre outras. A combinação com mais sucesso consiste no uso de biometrias e senhas ou chaves baseadas no conhecimento (p.ex: dados pessoais: telefone, código de endereçamento postal, data de nascimento, etc.).

A Fig.2.2 apresenta a tipologia de métodos de autenticação associada a sistemas baseados em características biométricas. Também mostra a autenticação com posses e conhecimento, sendo possível que um sistema trabalhe conjuntamente com esses parâmetros.

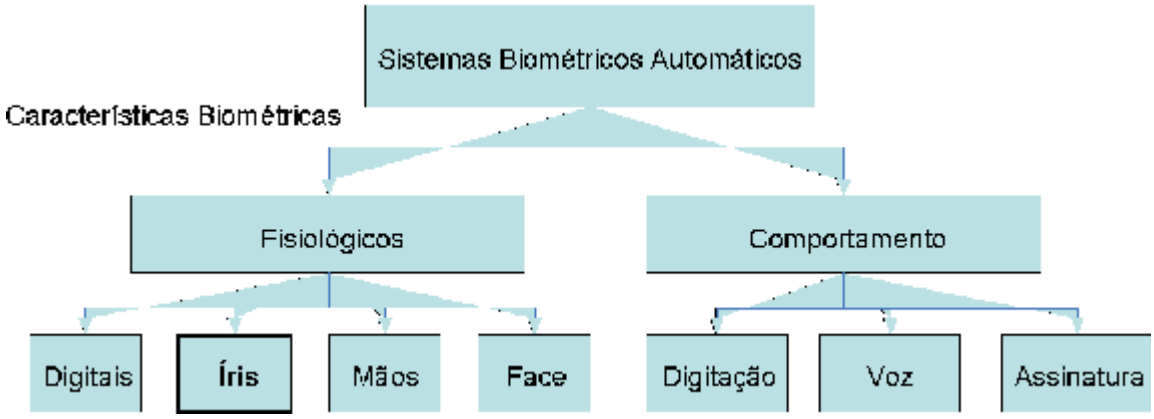


Fig. 2.2 Tipologia de métodos de autenticação associada a sistemas baseados características biométricas.

2.3 Reconhecimento de Padrões

Uma medida biométrica não é uma medida exata. Na verdade, ela varia com fatores externos, durante a aquisição de dados e com o passar do tempo, uma vez que os indivíduos mudam suas características fisiológicas e comportamentais ao longo de suas vidas. Isso resulta em um problema da biometria, pois ela está baseada nessas características variáveis. Esse fato está diretamente relacionado com o problema-chave já conhecido em **reconhecimento de padrões**, ou seja, a relação entre variabilidade intraclasse e a variabilidade interclasse.

A variabilidade intraclasse é a variabilidade entre instâncias diferentes de uma mesma classe, ou seja, a variabilidade presente em amostras de características fisiológicas ou comportamentais de um mesmo indivíduo.

A variabilidade interclasse, por sua vez, é a variabilidade entre instâncias de diferentes classes, ou seja, a variabilidade em amostras de características de indivíduos diferentes.

Dessa forma, uma medida biométrica ideal apresenta uma pequena variação intraclasse e uma grande variação interclasse. Isso tornaria baixas as taxas de falsa rejeição e falsa aceitação, tornando o sistema biométrico muito confiável para identificação pessoal (ver Fig. 2.3).

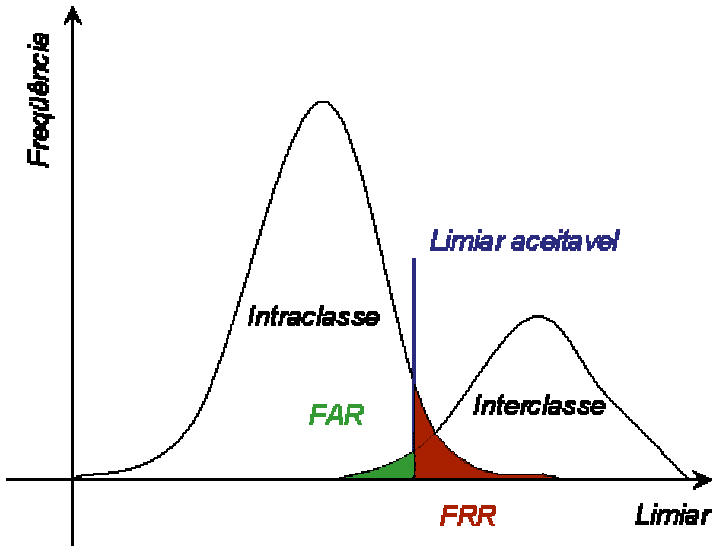


Fig. 2.3 A relação entre variabilidade intraclasse e a variabilidade interclasse da íris [w6].

Então, para obter um sistema seguro contra impostores são aplicados limiares um pouco mais baixos do que o normal, como se observa na Fig. 2.3, correspondente à biometria dos digitais.

2.4 Comportamentos Estatísticos da Biometria

2.4.1 FAR e FRR

A tarefa de identificação de um sistema biométrico tem relação com duas formas de resultado: aceitação e rejeição. O desempenho de um sistema pode, então, ser medido por duas taxas: FAR e FRR, descritos a seguir.

Taxa de falsa aceitação *(FAR - False Acceptation Rate)*, percentual de amostras de características de indivíduos diferentes erroneamente classificados pelo sistema como sendo de um mesmo indivíduo.

Taxa de falsa rejeição *(FRR - False Rejection Rate)*, percentual de amostras de características de um mesmo indivíduo erroneamente classificadas pelo sistema como sendo de outros indivíduos.

A FAR é definida como sendo a probabilidade de se aceitar um usuário quando se realiza uma medição para autenticação usando-se uma identidade que não corresponde ou até mesmo falsa. Nesse caso, o sistema aceita aquele usuário como verdadeiro. Isso pode acontecer porque o limiar operacional é ajustado demasiadamente baixo, ou porque as características biométricas de ambos são muito similares. Nesses casos, ocorre uma falsa

aceitação.

A importância da FAR está ligada ao algoritmo de classificação do padrão biométrico. Pode-se dizer que um algoritmo é seguro se praticamente não ocorre falsa aceitação.

A FRR é definida como a probabilidade de um usuário verdadeiro fazer uma tentativa de autenticação no sistema biométrico e ser rejeitado. Isso pode ocorrer porque o limiar operacional estimado para acesso é ajustado demasiadamente alto, ou porque a característica biométrica apresentada pelo usuário não é próxima o bastante do modelo armazenado (*template)* para o acesso. Nesses casos, há uma falsa rejeição.

A importância da FRR está ligada a robustez do algoritmo de classificação do padrão biométrico. Quanto mais preciso for o algoritmo, menor será o número de falsas rejeições [19]. Pode-se dizer que um algoritmo forte é aquele onde sempre que um usuário legítimo tenta autenticar-se, o sistema reconhece-o com sucesso.

A Fig.2.4 mostra esses dois parâmetros: FAR e FRR. .

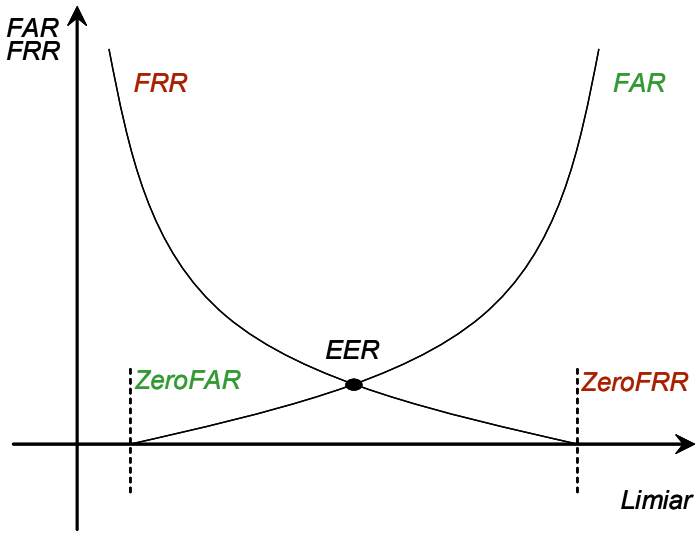


Fig. 2.4 Curvas FRR e FAR, sendo que a interseção é o ponto EER.

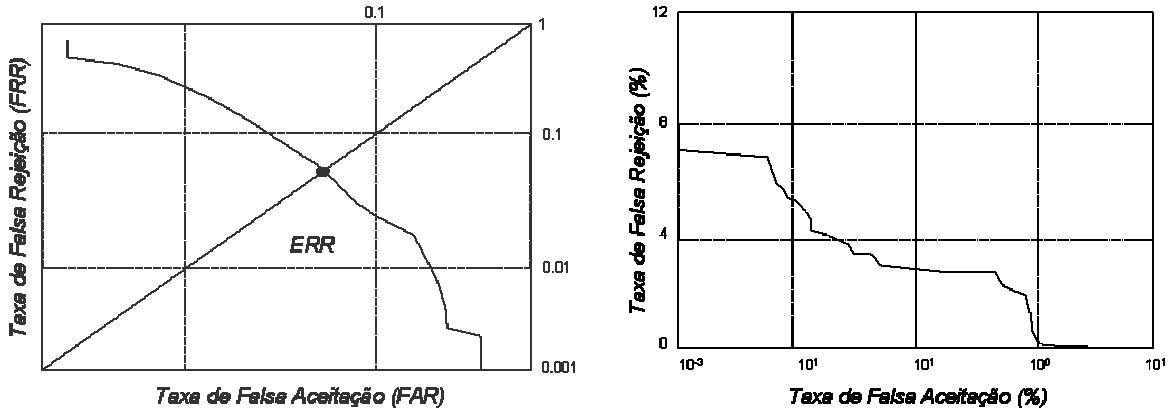
No caso ideal, existirão um ou mais pontos de referência, onde ambas as taxas de erro alcançadas seriam iguais ao zero. Na figura acima, pode-se observar três pontos importantes chamados de ZeroFAR, ERR (*Equal Error Rate*) e ZeroFRR.

ZeroFRR é o valor de FAR quando FRR tem valor zero e indica a probabilidade do sistema aceitar o acesso de pessoas não-autorizadas, quando todos os acessos de pessoas autorizadas são aceitas. ZeroFAR é o valor de FRR quando FAR tem valor zero e indica a probabilidade do sistema rejeitar o acesso de pessoas autorizadas, quando todos os acessos de pessoas não-autorizadas são rejeitados.

Neste trabalho aplicou-se um ZeroFAR que garanta um sistema seguro contra acessos não autorizados.

2.4.2 EER

EER é definido como o ponto de cruzamento entre os gráficos que contenham tanto a falsa aceitação quanto a falsa rejeição. Em outras palavras, é o ponto em que os valores de FAR e FRR são iguais. Segundo Ross [21], a taxa de erro igual (EER) é o ponto mais importante, pois especifica a separabilidade que o sistema oferece entre os acessos permitidos e os não-permitidos. O valor de EER pode ser calculado a partir de uma curva de características operacionais ROC (*Receiver Operating Characteristic*), podendo-se determinar a exatidão ou sensibilidade a erros de uma metodologia de autenticação biométrica.



(a) (b)

Fig. 2.5 Curvas ROC. (a) Uma curva genérica; (b) Uma específica de íris [29].

Para se calcular a curva de ROC de um sistema biométrico, cada um dos pontos correspondentes às curvas FAR e FRR é colocado em uma escala logarítmica (ver Fig. 2.5). O EER é encontrado traçando-se uma linha a 45 graus a partir do ponto de origem (0, 0). Onde essa linha cruza a curva ROC, está o ponto correspondente ao EER. Isso acontece porque quando a FRR tem valor igual a 1 (FRR = 100%), a FAR assume valor 0, e onde a FRR assume o valor 0, a FAR é igual a 1 (FAR = 100%). Em outras palavras, tem-se FAR=FRR.

Escolher o uso do ponto de cruzamento entre FRR e FAR é uma questão significante. Um EER calculado usando-se FRR e FAR é susceptível de ser manipulado, baseado na granularidade dos valores de limiares obtidos para a FAR e FRR. A importância do EER se dá quando se deseja comparar diferentes sistemas biométricos. De fato, cada sistema biométrico geralmente trabalha com seus próprios valores absolutos de limiares para se calcular FAR e FRR, dificultando a comparação direta. Porém, conhecendo-se o valor relativo de EER para um sistema, pode-se efetuar uma comparação estatística normalizada, embora em uma aplicação real um sistema de autenticação raramente consiga operar exatamente nesse ponto. Na prática, alguns sistemas são programados para trabalharem

próximos de ZeroFAR em casos de alta segurança enquanto que outros perto de ZeroFRR para conforto do usuário.

2.5 Formas de Aplicação da Biometria

2.5.1 Comparação, Verificação e Identificação

Um sistema de identificação deve conter subsistemas de verificação e de comparação. Isso, para se realizar a tarefa final de identificação de uma pessoa.

Os sistemas biométricos operam em dois modos: verificação e identificação. A identificação envolve comparação de um padrão (*template)* dentre todos os demais de uma base de dados. A verificação faz apenas uma comparação entre dois padrões [22]. Para o funcionamento prático em populações definidas, as bases de dados podem conter de centenas até milhões de registros. As bases de dados armazenam padrões ou vetores característicos das medidas biométricas.

A **comparação** de duas medidas biométricas consiste em se realizar uma medida de quão similar é uma da outra. No caso de **verificação** tem-se apenas uma medida biométrica e sabe-se a quem pertence. A função do sistema é verificar se essa medida corresponde a quem deveria pertencer. Isso é feito fazendo-se uma comparação da entrada com uma medida histórica armazenada. Uma **identificação** de uma entrada biométrica é uma tarefa longa, dado que é necessário se realizar uma procura em um histórico de medidas e verificar desde uma a muitas amostras a fim de fornecer como resposta o proprietário da medida. A seguir, apresentam-se as descrições de comparação, verificação e identificação orientadas a um sistema biométrico de íris automatizado digitalmente (ver Fig. 2.6).

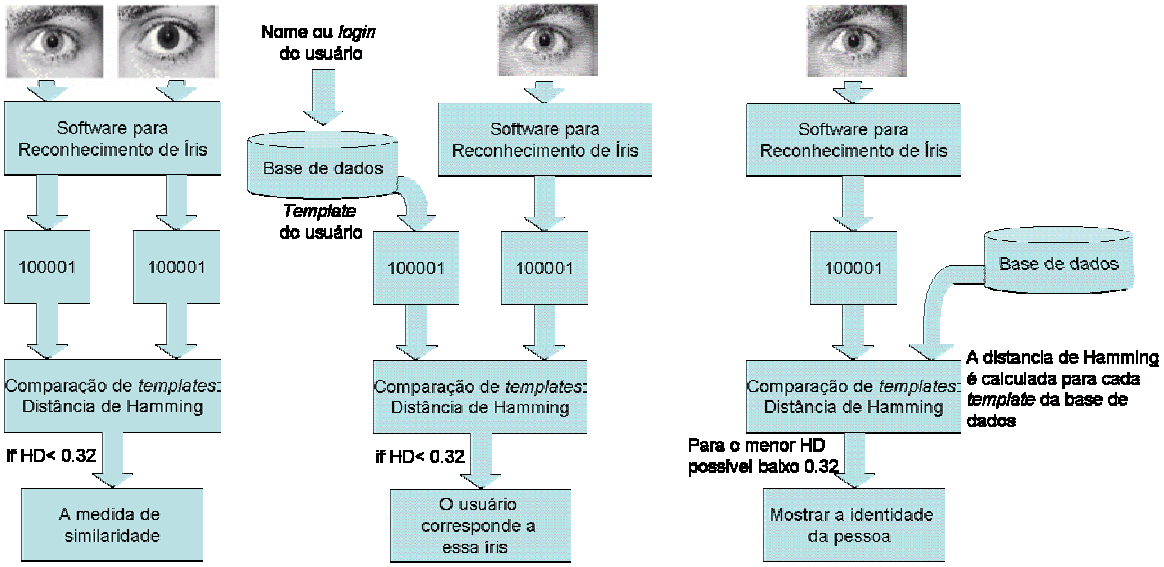


Fig. 2.6 Comparação, verificação e identificação de um sistema baseado em íris [30]

Comparação

Duas entradas biométricas de íris passam pelo dispositivo de captura e são processados pelo *software* associado. Após se gerar o vetor característico (*template*) para cada uma delas, comparam-se os mesmos usando-se a distância matemática HD (*Hamming Distance*). Se a distância for menor do que um limiar então as entradas são consideradas iguais senão são diferentes.

Verificação

A medida de íris e o nome ou *login* da pessoa são entradas do sistema. Uma base de dados procura o vetor característico associado ao nome da pessoa. Paralelamente a entrada biométrica é passada pelo dispositivo e processada pelo *software* associado, gerando-se assim o vetor característico de tal amostra. Ambos os vetores característicos, um da base de dados e outro gerado, são então comparados, como no item anterior. Termina-se a verificação quando a comparação fornece subsídios para a tomada de uma decisão. Nesse ponto sabe-se se a pessoa é quem disse ser.

Identificação

Deve-se entrar somente com medida de íris para se saber a quem corresponde essa entrada. Normalmente é feita uma verificação exaustiva do vetor característico de entrada e de outros vetores de toda a base de dados.

Finalmente, para que um sistema biométrico seja eficiente ele deve conter na interface do sistema essas três opções. O tempo de processamento e acesso à base de dados de uma identificação poderia ser, no pior dos casos, igual ao tempo de acesso por unidade multiplicado pela quantidade de registros da base de dados.

2.5.2 Classificação (*Screening*)

Nos sistemas biométricos, do tipo um para muitos (identificação), ocorrem problemas devido ao fato de que as bases de dados associadas contêm uma alta quantidade de amostras. Dessa forma, a tendência é a verificação de um para muitos, tornar-se demorada. Imagine-se, por exemplo, que o tempo de comparação de uma biometria demora 0,1 segundos. Então para uma base de dados simples que não seja relacional, o tempo de comparação corresponde ao tamanho da base de dados, ou seja, se ela contiver 1000 amostras, então poderia levar 100 segundos no pior caso.

A classificação (*screening*) tem como objetivo classificar e generalizar as amostras de uma base de dados biométrica de acordo com algum critério ou característica. O alvo dessa classificação pode ser a própria identificação (Fig. 2.7). No entanto, para reconhecimento de íris é necessário se gerar grupos com características similares onde uma distância HD (ou outra métrica) represente a todos do grupo e seja o mais diferenciado dos outros grupos.

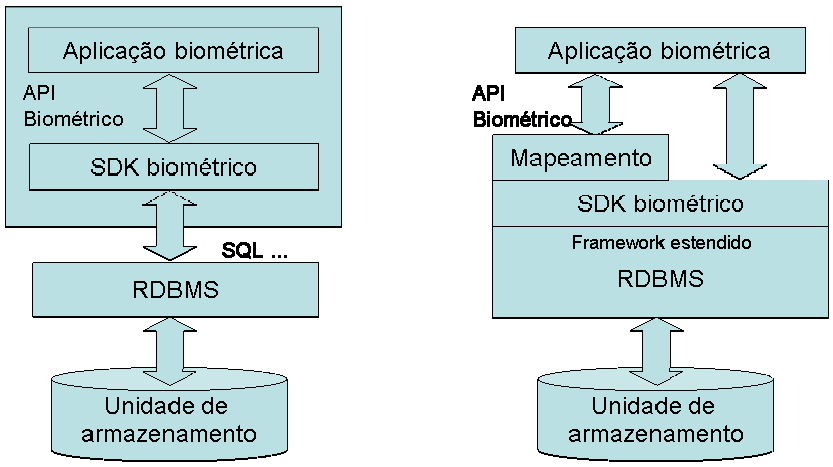


Fig. 2.7 Modelo experimental de classificador (*Biometric SDK*) para identificação no caso da *Oracle Corporation* [24]. (a) Modelo integrando a aplicação biométrica e o classificador; (b) Modelo integrando o classificador com o gerenciador de base de dados.

A classificação para reconhecimento de íris via redes neurais foi aplicada em [25] e [26], mas sem experimentos que avaliem o seu desempenho em comparação com os métodos por transformadas. Wang [23] usou redes neurais para uma classificação de animais (não fez identificação). De fato, esquemas de redes neurais [27] estão sendo utilizados como classificadores. Dessa forma, poderia também ser utilizado, se for especializado, para classificar íris *screening* e gerar representantes de possíveis grupos. Essa área de classificação [28] e exclusivamente para o reconhecimento de íris é pouco explorada, sendo um problema para se resolver no futuro.

Capítulo 3

Considerações para a Seleção de uma Biometria

3.1 Testes de Laboratório

O laboratório *UK National Physical Laboratory* [9] publica (*Test Report 2001*) resultados de testes de biometrias que são comercializados entre empresas. Dentre os resultados mais importantes e publicados livremente na internet encontram-se aqueles baseados em taxa de falsa aceitação e falsa rejeição. As curvas mostram que a íris obtém resultados ótimos (Ver Fig. 3.1).

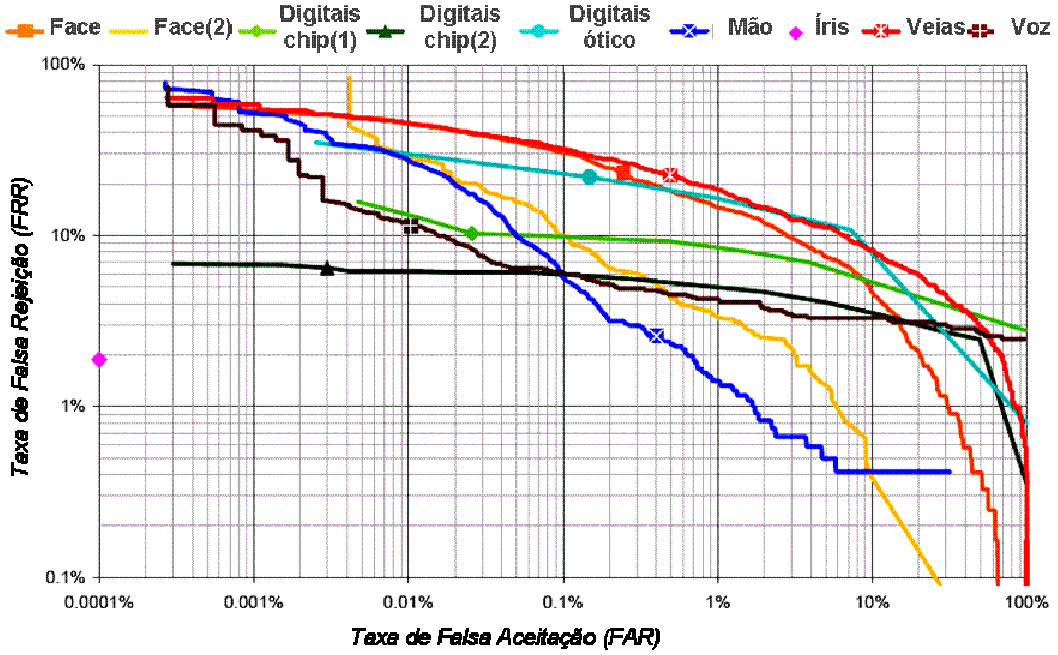


Fig. 3.1 Teste FAR vs. FRR. "*UK National Physical Laboratory Test Report 2001*" [9].

3.2 Os Três Fatores

Os três fatores constituem uma forma simples de comparação para se fazer uma escolha de uma biometria apropriada [31] (ver Tab. 3.1).

Característica	Descrição
Desempenho	Refere-se à capacidade de um sistema em autenticar corretamente um indivíduo devido a um tipo de características biométrica.
Aceitabilidade	Indica o grau de aceitação das pessoas em relação a esse tipo de identificação biométrica na sua vida cotidiana
Fraudabilidade	Reflete a facilidade com que um sistema pode ser enganado por métodos fraudulentos.

Tab. 3.1 Os fatores básicos para identificar uma biometria [31].

3.3 Critério utilizado por Autores na Literatura

Segundo J. Daugman para que uma característica biométrica tenha desempenho aceitável para identificação pessoal é desejável que [32]:

Característica	Descrição
Intraclasse	A variabilidade em um mesmo indivíduo seja mínima.
Interclasse	A variabilidade entre indivíduos distintos seja máxima.
Genética	A influência genética seja a menor possível.
Aleatória	A aleatoriedade seja muito alta.
Estável	A estabilidade seja muito alta ao longo da vida.

Tab. 3.2 Critério de Daugman para escolha de uma biometria.

Essas características estão presentes em uma biometria baseada em íris e correspondem a uma genética e aleatoriedade como propriedades fortes o que outras biometrias não possuem. Outra forma de mostrar o desempenho de uma biometria é a experimentação. Embora seja difícil realizar para cada uma das biometrias, o algoritmo de Daugman baseado em íris foi testado e os resultados comprovam que se trata de uma ótima biometria (ver Tab. 5.1).

M. Bromba [33] apresenta uma tabela avaliando as biometrias, baseando-se em vários fatores (ver Tab. 3.3).

Biometria	Conforto	Exatidão	Disponibilidade	Custo
Digitais	ooooooo	ooooooo	oooo	ooo
Assinatura	ooo	oooo	ooooo	oooo
Face	ooooooooo	oooo	ooooooo	ooooo
Íris	oooooooo	ooooooooo	oooooooo	oooooooo
Retina	oooooo	oooooooo	ooooo	ooooooo
Geometria da Mão	oooooo	ooooo	oooooo	ooooo
Veias da mão.	oooooo	oooooo	oooooo	ooooo
Forma da orelha	ooooo	oooo	ooooooo	ooooo
Voz	oooo	oo	ooo	oo
DNA	o	ooooooo	ooooooooo	ooooooooo
Odor	?	oo	ooooooo	?
Digitação.	oooo	o	oo	o
Password	**ooooo**	**oo**	**oooooooo**	**o**

Tab. 3.3 Critério segundo M. Bromba [33] (= bom; =ruim.)

Cada um desses valores foi analisado pelo autor e associou-se uma pontuação. Também se observa uma seleção das melhores características de acordo com os padrões mostrados na Tab. 3.3. Destaca-se a face e a íris como sendo boas biometrias. O DNA também constitui uma boa biometria, mas com pontuações muito ruins em custo e conforto. A biometria de menor custo é a dinâmica de digitação, porém apresenta problemas em relação à disponibilidade e à falta de exatidão quando comparado com outras biometrias tais como a íris.

3.4 Os Sete Pilares

As características biométricas incluem vários subconjuntos de características relacionadas com o corpo humano, mas nem todos são adequados para se identificar populações. É desejável que as características particulares escolhidas para uso em biometria satisfaçam os sete pilares [34] apresentados na Tab. 3.4.

Característica	Descrição
Universalidade	Todos os humanos são dotados de uma característica física comum, que pode ser usada para identificação.
Distinguibilidade	Cada pessoa tem características únicas, que permitem a diferenciação entre as pessoas.
Imutabilidade	Algumas características mudam depois de um longo tempo ou não mudam durante a vida de uma pessoa.
Facilidade de uso	A característica pode ser coletada de forma razoavelmente fácil visando uma identificação rápida.
Desempenho	Depende do grau de exatidão de identificação.
Aceitabilidade	As aplicações não alcançam sucesso se o público discorda ou se resiste à biometria.
Resistência a casos de fraude	Para aumentar a segurança, os sistemas necessitam de um gerenciamento de identidade resistente à possíveis fraudes.

Tab. 3.4 Os sete pilares de Wisdom [34]

3.5 Pontuação por Característica

A pontuação por característica é uma recomendação para ambientes de segurança [35]. Avaliam-se as características de biometrias escolhidas e testadas, a fim de se examinar os pontos fortes e fracos (*strengths & weakness*).

Essa recomendação serve para examinar as biometrias aplicáveis em ambientes de segurança bem como suas qualidades associadas. A escolha de uma tecnologia apropriada deve levar em conta as necessidades pertinentes à aplicação específica bem como os itens necessários à construção do sistema. A recomendação é feita supondo-se que as melhores tecnologias estejam disponíveis. Essa recomendação deve ser analisada e revisada caso a

tecnologia necessária seja muito avançada. As características relevantes para se determinar uma biometria apropriada para um ambiente de segurança são apresentadas na Tab. 3.5.

Característica	Pontuação (min: 0, max: 10)
Acceptance	Aceitação do usuário**.**
Easy	Facilidade de utilização.
ROI	Custo da tecnologia.
Deployability	Disponibilidade.
Noninvasive	Invasibilidade da tecnologia.
Maturity	Maturidade da tecnologia.
FAR, FRR, *Size*	As taxas de falsa aceitação e rejeição e o tamanho adequado.
Habituation	O tempo de adequação para o usuário se sentir habituado.

Tab. 3.5 Características para avaliação e pontuação [35].

Cada característica será brevemente descrita a seguir.

3.5.1 Aceitação do Usuário (*Acceptance*)

A aceitação do usuário em se submeter à tecnologia biométrica usada decide o sucesso da aplicação de um sistema biométrico escolhido. A aceitabilidade de uma biometria pode ser medida usando-se medidas quantificáveis. Essas medidas de aceitabilidade que são quantificáveis, são:

- Número de chamadas ao módulo *help* ou de ajuda.
- Número de tentativas realizadas e tempo de autenticação por usuário.
- Número de vezes de chamadas ao módulo de *'fallback'* de autenticação.

Para uma avaliação inicial, o fato de se ter alta incidência nas chamadas de ajuda é uma medida negativa indicando que o sistema apresenta-se complexo para o usuário. Em relação ao tempo de autenticação, este pode ser muito variável dependendo da biometria utilizada. Pode-se dizer que o tempo de medida será curto ou a espera será longa dependendo de fatores relacionados com as exigências do usuário final e com a aplicação da biometria. Esse fato influencia no grau de aceitação do usuário. Por exemplo, uma longa espera poderia ser aceitável para a entrada de um usuário a um módulo de caixa bancário, mas não seria aplicável para um *'login'* em uma escola.

O recurso de *fallback* atende às situações que são mais complexas. Por exemplo, dependendo do tipo de falha de autenticação, o sistema se reiniciará ou então bloqueará o processo de identificação. Isso pode ser implantado no sistema devido à necessidade de

segurança ou para se tratar diversos tipos de erro de entrada. Além disso, o sistema deverá estar adequado a aquela parte da população que apresente alguma razão fisiológica, psicológica ou religiosa a fim de atender às exigências legais do país ou simplesmente do cliente desejado. Deve-se considerar também que as respostas ao uso das tecnologias biométricas variam de acordo com a habilidade e comportamento das pessoas, bem como com o treinamento. Para todos esses casos, o sistema deverá ter a capacidade de usar algum recurso de *fallback*, sabendo-se que se a biometria for adequada, será menor o uso desse módulo.

3.5.2 Facilidade de Utilização (*Easy*)

Em geral, o sucesso de alguma tecnologia depende diretamente da facilidade de uso. Se uma tecnologia é de difícil uso, então os consumidores tendem a não comprar tal tecnologia. As empresas, na finalização de um produto, têm gastado tempo e recursos na consideração desse aspecto. Na área de biometria, em termos de facilidade, é necessário ter em consideração o seguinte:

- Ergonomia.
- FRR.
- *Software* biométrico.

A ergonomia está associada à facilidade de uso, segundo as empresas. Descreve a relação da interação humana com o produto. A ergonomia em biometria dá mais importância à facilidade de utilização. Os dispositivos biométricos devem trabalhar com as pessoas de forma a mais natural possível. Outro aspecto de facilidade de uso é a FRR que depende do algoritmo utilizado. Se o algoritmo causa uma FRR alta, então o sistema não será de fácil uso. Muitas tentativas e rejeições sucessivas podem produzir frustração e falta de aceitação no usuário. Outro aspecto refere-se ao *software* de controle do sistema biométrico onde também é desejável uma interface de fácil uso.

3.5.3 Disponibilidade (*Deployability*)

Antes de se escolher uma biometria, o interessado (empresa, firma, estabelecimento, etc.) que utilizará a mesma deve saber se essa tecnologia está disponível e se tem suporte técnico. Isso é necessário para se realizar eventuais correções de erros, adaptações e manutenções rápidas. Dessa forma, mesmo que a solução proposta seja adequada e aceita pelos usuários, pode não ser praticável se não estiver disponível.

3.5.4 Custo da Tecnologia (*ROI*)

O custo não é tão importante como o é a facilidade de uso da biometria, mas de fato,

uma biometria que fosse muito custosa restringiria seu campo de aplicação. O custo de uma tecnologia biométrica está baseado em:

- Custo do dispositivo.
- Custo do projeto de aplicação.
- Suporte e manutenção.

O custo do dispositivo varia de acordo com a biometria utilizada e deveria abranger a funcionalidade e a robustez do sistema (mais investimentos tendem a produzir melhores resultados). No entanto, o custo efetivo de uma apropriada biometria está no projeto de aplicação do sistema. Inclui tanto o *software* e *hardware* de todo um sistema quanto os servidores e a implantação da rede.

Os custos de manutenção e suporte estão associados às possíveis falhas dos dispositivos ou à melhoria de tecnologias com o passar do tempo. Se as falhas e os custos de suporte aumentam, então o retorno de investimento ROI (*Return of Investment*) decresce.

Uma biometria apropriada deve ter um suporte fácil bem como oferecer flexibilidade em *hardware* e *software*.

3.5.5 Tecnologia Não Invasiva (*Noninvasive*)

Do ponto de vista dos usuários uma biometria apropriada não deve ser invasiva. A medida do grau de invasão de um dispositivo pode ser o nível de envolvimento do usuário no funcionamento do sistema.

(a) (b) (c)

Fig. 3.2 Graus de invasibilidade (a) Baixo [36]; (b) Médio [37]; (c) Alto [38].

A leitura da íris ainda é vista como algo invasivo, pois é difícil para muitas pessoas se sentirem confortáveis com os procedimentos necessários. Na Fig. 3.2, observam-se diversos tipos de tecnologias biométricas de íris [36], [37], [38]. Uma biometria apropriada deveria ter um grau de invasão mínimo quando uma característica do usuário é medida.

3.5.6 Maturidade da Tecnologia (*Maturity*)

Quando se escolhe um sistema biométrico para uma dada necessidade, primeiro verifica-se a disponibilidade dele no mercado. É razoável assumir que uma tecnologia tem maturidade se foi testada no mercado e comparada pelos usuários com outras tecnologias. Além disso, em geral as gerações mais recentes de produtos apresentam melhorias em relação ao tamanho, ao custo ou à ergonomia. O custo também tende a decrescer se na fabricação são melhorados os processos internos. Por outro lado, a adição de mais recursos tende a aumentar o custo. Encontrar um ponto de equilíbrio, onde a tecnologia tem um custo compatível com as funcionalidades necessárias, somente será possível se essa tecnologia tem maturidade. A maturidade facilita o atendimento das condições do projeto dentro de um orçamento disponível.

3.5.7 Tempo de Adaptação (*Habituation*).

O uso progressivo de um sistema biométrico, onde os usuários se habituam de modo progressivo e positivo com o sistema, pode levar ao sucesso da biometria implantada. Se essa característica de adaptação estiver presente, isso aumentará o conforto do usuário. A seleção de um dispositivo deve ter influência na rápida adaptação do usuário. As chances de sucesso aumentam se houver combinação com facilidade de uso, maturidade e ergonomia.

Dessa forma, uma biometria apropriada deve apresentar características bem como ergonomia que ajudem ao usuário a acostumar-se com comodidade ao seu uso.

3.6 Desafio, Fabricação e Aplicações *(Issues and Challenges*)

Os sistemas biométricos atuais podem ser classificados, de acordo com sua funcionalidade, em dois grupos principais: sistemas de verificação e sistemas de reconhecimento. Nos sistemas de verificação, a pessoa que está sendo identificada afirma possuir determinada característica. Logo, o sistema deverá apenas aceitar ou rejeitar tal afirmação e, para tanto, ele deverá realizar uma comparação do tipo "um para muitos". Já nos sistemas de reconhecimento, a identificação da pessoa é feita a partir de uma busca em uma base de dados cadastrada previamente. O sistema percorre essa base até encontrar um indivíduo que apresente um conjunto de características semelhantes a aquelas apresentadas realizando, nesse caso, uma comparação do tipo "um para um". Os sistemas biométricos podem ser usados em qualquer situação que requeira uma resposta rápida e correta para a questão "*Quem é você*?". Uma das grandes vantagens dos sistemas biométricos sobre os

sistemas de identificação tradicional baseados em senhas, cartões de acesso, registro de identificação geral RG, e outros é que, nesses sistemas, o reconhecimento baseia-se em aspectos intrínsecos ao ser humano. Os sistemas de reconhecimento que não são baseados nesses aspectos intrínsecos nem sempre são seguros. Por exemplo, chaves e cartões de acesso entre outros podem ser perdidos, duplicados ou roubados. Senhas, códigos secretos e números de identificação pessoal podem ser facilmente esquecidos, compartilhados ou observados por outrem. Os sistemas biométricos, por outro lado, são menos vulneráveis a tais problemas. Porém todas essas características criam um desafio, isto é, a aplicação deve ser viabilizada a custos factíveis para os interessados. A implementação de tais sistemas inclui vários problemas em conjunto e deve satisfazer as expectativas dos usuários finais e dos demais envolvidos. Isso corresponde ao desafio de se criar e projetar sistemas que usando diversos dispositivos disponíveis solucionem esse conjunto de problemas. Depois de projetado um sistema próximo ao ideal, a fase de fabricação corresponde a um outro problema que deve levar em conta o custo. A otimização do custo depende tanto do local de utilização quanto da forma de aplicação e naturalmente não se pode esquecer dos fatores ambientais (ver Tab. 3.6).

Fator ambiental	**Íris**	**Face**	**Digitais ópticos**	**Digitais CMOS**	**Geometria da mão**	**Voz**
Iluminação	X	X	X		X	
Níveis de sons						X
Temperatura			X	X	X	
Ruído branco	X	X	X	X	X	X
Umidade			X	X		
Impurezas	X	X	X		X	
Variação de linha de tensão	X	X	X	X	X	X
Vibração	**X**	**X**	**X**	**X**	**X**	**X**

Tab. 3.6 Fatores ambientais que afetam uma tecnologia biométrica [39]
CMOS - *Complementary Metal Oxide Semiconductor*.

Capítulo 4

Tecnologias Biométricas

As tecnologias biométricas apresentadas neste capítulo exploram características físicas que permitem reconhecimentos de face, de digitais, de DNA, de geometria da mão e de íris. Também podem aproveitar características de comportamento que possibilitam, por exemplo, a verificação da identidade através da voz.

A arquitetura de um sistema biométrico genérico descrito em [8] contém seis passos básicos:

- Captura de amostra. Esse passo utiliza um sensor apropriado ou dispositivo para recolher amostras biométricas.
- Extração de características. Esse passo transforma a amostra de entrada em um *template* ou vetor característico. Normalmente trata-se de um dado numérico.
- Qualidade de verificação. Esse passo estabelece se a comparação de um *template* com a entrada capturada está correta.
- Armazenamento de *template*. Esse passo registra um *template* em algum espaço volumétrico de armazenamento e depende dos requisitos de aplicação.
- Casamento (*matching*). Nesse passo compara-se em tempo real, uma entrada correspondente a um indivíduo com um *template* armazenado.
- Decisão. Esse passo é o resultado do casamento que esteja em concordância com algum critério de aplicação.

Conforme se observa somente os dois últimos passos, isto é, o casamento e a decisão são utilizados na fase de reconhecimento.

A seguir apresenta-se uma breve descrição das principais tecnologias biométricas usadas.

4.1 Reconhecimento Facial

Uma das áreas que cresce mais rapidamente na indústria da biometria em termos de novos esforços de desenvolvimento é a identificação pessoal através da verificação da face [17]. Muitos dos trabalhos nessa área empregam tanto métodos de redes neurais quanto correlações estatísticas de formato geométrico da face (ver Fig.4.1).

Fig. 4.2 Reconhecimento facial [20].

Esses métodos tentam imitar como os seres humanos reconhecem uma outra pessoa. A imagem das faces é adquirida de forma direta pelos equipamentos de vídeo que hoje em dia estão disponíveis. Os atuais sistemas têm dificuldade de conseguir altos níveis de desempenho quando a base de dados aumenta a quantidade de informação para alguns milhares de indivíduos [40].

4.2 Reconhecimento de Digitais

A estabilidade e unicidade das impressões digitais são bem reconhecidas pela sociedade. Segundo Wayman [17], estima-se que a chance de duas pessoas, incluindo gêmeos, terem a mesma impressão digital é menor do que uma em um bilhão. As tecnologias baseadas em impressões digitais são de longe as mais utilizadas atualmente [41]. A extração de características sobre impressões digitais se baseia em encontrar a posição de pequenos pontos chamados de minúcias que estão presentes nas digitais, tais como, pontos de finalização de linhas e pontos de junção de linhas (ver Fig.4.2).

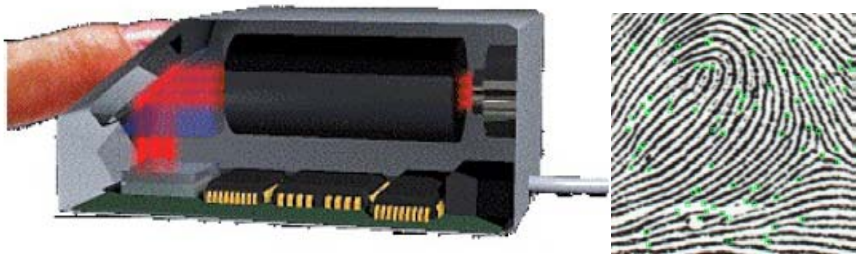


Fig. 4.4 Digitais [w9], [w10].

Outros métodos contam o número de vales e sulcos que existem entre esses pontos [41]. Dependendo do esquema de identificação escolhido e do grau de segurança do sistema, o arquivo de referência que contem as informações sobre a impressão digital varia de algumas centenas de bytes até milhares de bytes. Hoje em dia, a maior aplicação da tecnologia de impressões digitais é em sistemas de identificação automática utilizadas pela polícia em vários países do mundo.

Essas características, normalmente, se desenvolvem nas mãos e pés, alguns meses antes do nascimento e permanecem constantes durante a vida, a menos que se sofra algum corte ou machucado acidental [43].

Um intenso trabalho manual pode causar variações consideráveis nas digitais. Por outro lado, um dispositivo de captura da imagem pode ficar sujo, oleoso e encardido uma vez que é necessário um contato direto com o dedo. Esses fatos interferem na qualidade de imagem e pode provocar erros consideráveis [44].

Há uma possibilidade de resistência dos usuários em fornecer as digitais, devido ao fato de que, historicamente, as impressões digitais eram usadas por agências de execução de lei para identificar criminosos. Além disso, algumas pessoas, por questões de higiene, têm receio em colocar o dedo no dispositivo de captura que foi tocado por muitas pessoas estranhas [43].

4.3 Verificação de DNA

Uma identificação de uma pessoa através de seu DNA pode ser obtida através de amostras de sangue, saliva, cabelo ou pele. As características da seqüência de proteínas de várias sessões da cadeia de DNA são analisadas para se gerar um perfil de DNA que é comparado com outros perfis para se avaliar o grau de coincidência (ver).

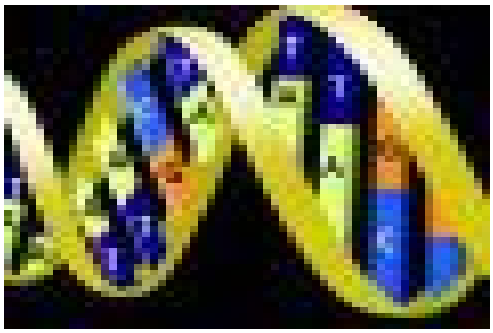


Fig. 4.6 DNA [46].

O DNA possibilita uma característica biométrica poderosa, sendo freqüente a opinião de que o uso de DNA fornece um melhor desempenho biométrico com respeito ao FAR e ao FRR. Entretanto, além do tempo que se consome durante o procedimento de análise que envolve manipulações físico-químicas, há dois problemas: primeiro, os métodos de análise de DNA usados hoje não podem distinguir entre gêmeos monozigotos [45]. Essa é uma limitação principalmente às aplicações forenses, não sendo em geral uma restrição forte para as aplicações comuns, mas influencia as taxas de erro médias.

Atualmente uma análise de DNA pode ser indicada para verificação de paternidade ou para comprovação de circunstâncias quando autorizada pela legislação. Quase todos os estados norte-americanos obtêm amostras de DNA dos presidiários e criminosos violentos, e em quatro estados toma-se o DNA de todos os presidiários, segundo artigos mencionados no *DNA Resource* [46]. A base de dados, do FBI (*Federal Bureau of Investigation*), contém mais de 2,1 milhões de amostras. Mas a análise de amostras toma várias horas e falta muito ainda para o procedimento vir a ser utilizado regularmente, segundo Maud Meister, consultor do *International Biometric Group - New York* [47].

4.4 Identificação e Verificação de Voz

A voz é utilizada em sistemas automáticos de identificação de locutor (ver). Essa abordagem biométrica é muito atrativa visto que ela é pouco invasiva, segundo considerado pelos usuários.

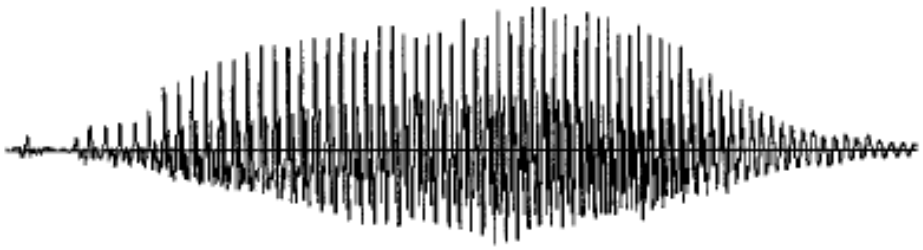


Fig. 4.8 Verificação de voz [48].

Os humanos utilizam fenômenos de alto nível [17], tais como sotaque, estilo do locutor, entonação, estado emocional, dentre outros, para reconhecer uma pessoa através de sua voz. No entanto, esse tipo de característica é difícil de ser adquirido e mensurado de forma automática pelo computador. Usam-se assim parâmetros de baixo nível derivados de medidas acústicas do sinal de voz tais como, freqüência fundamental, envoltória espectral, freqüência de formantes e energia, entre outros.

4.5 Reconhecimento de Assinaturas

Os sistemas de reconhecimento de assinaturas se dividem em sistemas dinâmicos e sistemas estáticos (ver). Os sistemas dinâmicos de reconhecimento de assinaturas utilizam técnicas baseadas nas pequenas diferenças do processo dinâmico da escrita da assinatura, como por exemplo, pressão, aceleração, e número de vezes que se levanta a caneta do papel. Por outro lado, os sistemas que utilizam apenas a imagem da assinatura (sistemas estáticos), utilizam características como uma inclinação dos traços da escrita, o número de palavras bem como a razão entre a altura e o comprimento da assinatura [17].

Fig. 4.10 Reconhecimento de assinatura.

A chave do sucesso de um sistema de identificação de assinaturas consiste em se encontrar características de assinatura que sejam mais constantes, isto é, que variem pouco durante o processo de cadastramento.

4.6 Verificação de Geometria da Mão

A autenticação em um sistema de identificação através de geometria da mão baseia-se em medidas das dimensões de partes da mão, tais como comprimentos de dedos, sua largura e também a área. A classificação utilizando-se esses parâmetros, leva em conta a forte correlação que existe entre essas diferentes medidas. Os primeiros sistemas baseados nessas características datam de 1960, sendo que as medidas que utilizavam correspondiam apenas aos comprimentos de quatro dedos [17].

Fig. 4.12 Geometria da mão [w12].

4.7 Reconhecimento de Olho: Íris e Retina

A tecnologia de reconhecimento através do uso de retina captura e analisa os padrões dos vasos sanguíneos do nervo fino posicionado na parte posterior do globo ocular [50]. Os padrões da retina são traços altamente distintos entre as pessoas obtendo uma exatidão de 1 para 10 milhões [49]. Esse padrão permanece estável por toda a vida de uma pessoa, mas pode vir a ser afetado por doenças. O fato de a retina ser pequena e estar posicionada no interior do olho dificulta o procedimento de captura da imagem, já que é necessário ao usuário olhar fixamente para um ponto imóvel até que a câmera focalize os padrões e, assim, os capture adequadamente (ver Fig. 4.13).

Fig. 4.13 Reconhecimento de íris e veias da retina [w13].

Tanto o padrão da íris quanto o padrão dos vasos sangüíneos do fundo do olho (retina) provêem uma base única para identificação [17]. A principal vantagem da captura do padrão da íris sobre a varredura da retina é que na primeira não se necessita que o olho do indivíduo que está sendo testado esteja focalizado em um determinado lugar. Também a íris não sofre nenhuma alteração devido a doenças como ocorre com a retina [51]. Ainda mais, segundo [52], a imagem da íris pode ser obtida pelo dispositivo de captura até a uma distância de cerca de um metro. Cada olho tem seus próprios padrões totalmente distintos na formação dos vasos sanguíneos, mesmo em olhos de gêmeos idênticos. Essa medida é realizada direcionando-se uma luz infravermelha de baixa intensidade na pupila e na parte posterior do olho. O padrão da retina é refletido de volta para a câmera, a qual captura a imagem. A varredura da retina é um dos melhores métodos biométricos existentes, com taxas de erro pequenas, base pequena de dados de referências e processos rápidos de confirmação de identidade. O que mais dificulta a difusão desse tipo de tecnologia continua sendo ainda a resistência dos usuários, isto é, convencer a pessoa que vai se servir dessa técnica para a autenticação de identidade, de que a luz infravermelha que incidirá sobre seu olho não lhe irá fazer mal [17]. No capítulo seguinte são ampliadas as informações de características de íris que são usadas em biometria.

4.8 Dinâmica de Digitação

A dinâmica de digitação, também chamada de ritmo de digitação, fornece um método biométrico que está diretamente ligado a área de segurança de computadores. Como o nome indica, esse método analisa a maneira como os usuários digitam no teclado seu *login* e sua senha (ver Fig.4.8). Nesse caso, as características extraídas são as seqüências de valores alfanuméricos que se está digitando, assim como o intervalo de tempo entre apertar uma tecla e outra para se compor uma palavra [53].

Fig. 4.14 Dinâmica de digitação para acesso no computador.

No passado, foi observado que os operadores de telégrafo possuíam uma maneira particular de digitar as mensagens. De fato, era possível para outros operadores identificarem quem estava transmitindo a mensagem apenas escutando o som da digitação de pontos. Durante o ato de digitar sua senha, os usuários desses sistemas protegidos certamente [54] impõem um ritmo quando pressionam e soltam as teclas, gerando um ritmo dinâmico de digitação das senhas [18].

Na maioria das vezes, as características biométricas de dinâmica de digitação são extraídas do sinal baseado nos tempos dedicados a cada uma das teclas digitadas por um indivíduo durante a digitação de uma palavra chave, frase ou texto [18].

4.9 Sistemas Biométricos Multimodais

As limitações de sistemas biométricos unimodais (ou seja, toma-se uma característica biométrica) como daqueles descritos anteriormente podem ser contornadas usando-se sistemas biométricos que trabalham com várias características biométricas (ou vários modos) simultaneamente. Tais sistemas são chamados de multimodais [55]. Os sistemas biométricos multimodais utilizam múltiplos dispositivos para capturar diferentes tipos de biometrias. A integração de dois ou mais tipos de biometrias quando bem combinados [56] aumenta o desempenho do sistema híbrido. Normalmente, os sistemas biométricos multimodais, procuram complementar uma biometria com outra a fim de minimizar os pontos fracos e maximizar os pontos fortes. Os sistemas biométricos multimodais podem ser implementados com diferentes tipos de recursos, tais como: sistemas com sensores múltiplos (digital e íris), medidas biométricas múltiplas (íris e o rosto), unidades da mesma biometria (formato e textura do rosto), amostras múltiplas de uma biometria (íris, várias vezes) e representação múltipla para que os algoritmos de casamento identifiquem à biometria (*iriscode* e *ICA*) [57]. A fusão para um casamento satisfatório de diferentes biometrias é relativamente simples se os valores de similaridade das diferentes modalidades são adequadamente combinados [58].

Nesse tipo de sistemas o custo aumenta, mas tem-se um ganho em relação à

confiabilidade. Combinando-se tecnologias biométricas que sejam confiáveis garante-se o sucesso de tais sistemas. A tarefa, portanto consiste em se determinar sistemas que tenham características confiáveis e que sejam de baixo custo para serem aplicáveis em diversos ambientes. Assim, a tendência é utilizar esse tipo de esquema. Como se observa na Fig. 4.15, a tecnologia com biometria múltipla já obtém 2.9% do total de aplicações biométricas. Isso representa uma derivada positiva em termos de crescimento em relação às tecnologias biométricas.

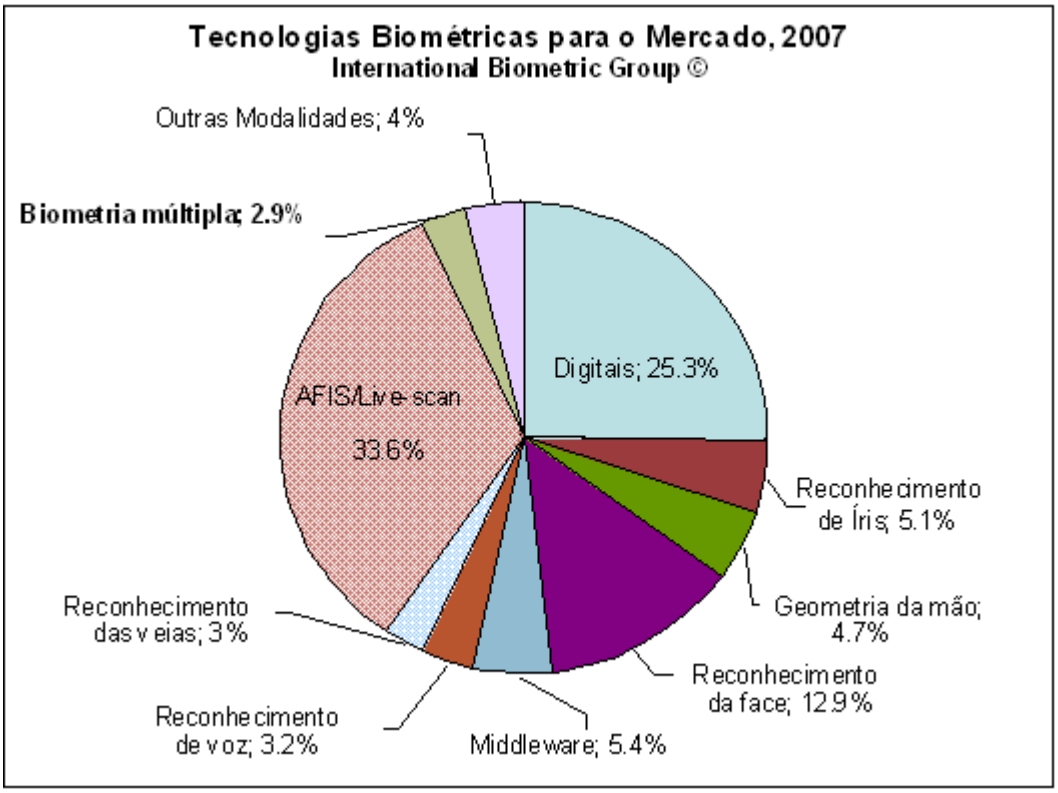


Fig. 4.15 Estado atual das tecnologias biométricas no mercado [47].

4.10 Comparação e Seleção de uma Biometria

Para se escolher uma biometria adequada podem-se utilizar os critérios observados no capítulo anterior. Entretanto, o critério deve ser adequado de acordo com a aplicação.

As avaliações gerais foram apresentadas no capítulo anterior e no Apêndice A onde se conclui que a íris, os digitais e a retina constituem biometrias ótimas. Entre essas biometrias, o uso de íris tem avançado mais em termos de segurança, diminuição do grau de invasibilidade, disponibilidade e aceitação do usuário [8], [9]. Assim, neste trabalho escolheu-se a íris como a biometria a ser usada por ter resultados e aplicações superiores comercialmente [8], [9], [10] .

Capítulo 5

Sistemas de Reconhecimento de Íris

5.1 Características da Íris Humana

A íris é um órgão interno que faz parte do globo ocular protegido pela córnea do olho, sendo colorida e cuja função é controlar os níveis de luz assim como faz o diafragma de uma câmera fotográfica. A pupila é a abertura para a entrada de luz que é controlada pela íris [81].

A descrição a seguir pode ser encontrada em boa parte nos trabalhos de dissertação de D. Ferreira e da M. Pereira [15], [84].

A íris tem características que são próprias de cada pessoa [52]. Existem muitos tipos de características combinadas com diversas cores (ver Fig 5.1). Durante o processo de envelhecimento, a partir de certa idade, a íris não se altera biometricamente, sendo isso uma de suas características fisiológicas mais importantes. A íris é formada no início da gravidez durante os três primeiros meses de gestação. Sua estrutura é completada aos oito meses e após esse tempo ocorrem algumas mudanças de textura. Aos dois ou três anos de idade ela deixa de mudar [51], [w26]. A formação da íris depende do meio no qual é formado o embrião. Dessa forma, muitos de seus detalhes não têm correlação com a carga genética [37], [61]. Cada pessoa possui uma íris diferente, sendo que isso ocorre mesmo que se trate de gêmeos univitelinos [6], [96]. Os órgãos do olho, o humor aquoso e a córnea protegem a íris do ambiente como se pode observar na Fig. 5.2. Essa proteção impede ou dificulta a mudança das características da íris. Evita também a ocorrência de riscos de lesão graves.

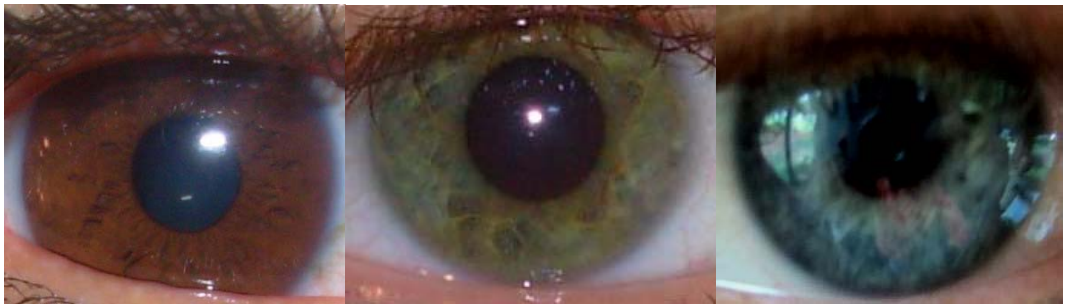


Fig. 5.1 Alguns tipos de íris.

Características da íris utilizadas para biometria

A estrutura microscópica da íris apresenta vários aspectos incomuns. Sua superfície anterior que forma o limite posterior da câmara anterior não é revestida por um epitélio distinto. O estroma contém vasos sanguíneos e nervos da região. Próximo da periferia da pupila, um conjunto de fibras musculares lisas forma uma estrutura contráctil anular, conhecido como esfíncter da pupila. A face posterior da íris consiste de um prolongamento das mesmas duas camadas de epitélio que revestem o corpo ciliar (células pigmentadas). A essa estrutura estão estreitamente associadas fibras lisas do dilatador da pupila, que estão dispostas radialmente. Existem depressões ou criptas, através das quais os vasos podem ser vistos no estroma. Há também várias pregas e estrias radiais ou circulares. A observação clínica da íris (realizada por oftalmologistas e anatomistas durante um período em que examinaram uma grande quantidade de olhos) permite afirmar que o padrão detalhado de uma íris é único. Isso ocorre ainda que se trate da íris esquerda ou da direita de um mesmo indivíduo. O padrão de uma determinada íris varia muito pouco [6], [96].

(a) (b)

Fig. 5.2 Olho humano. (a) Características circulares e angulares da íris [37]; (b) Anatomia do olho [81].

Por outro lado, constatou-se que raramente o processo evolutivo transcorre de forma inadequada, dando origem a uma íris rudimentar ("aniridia") ou a uma distorção na forma da pupila ("colobloma"). Evidências evolucionistas também tendem a comprovar a estabilidade do padrão da íris no tempo. Determinadas partes da íris já se encontram desenvolvidas no nascimento, enquanto que outras, tais como a fina musculação desenvolve-se durante os primeiros dois anos de vida. De particular importância para o reconhecimento de padrões, é o fato de que a pigmentação da íris continua até a adolescência. Na verdade, o tamanho médio da pupila sofre pequenos acréscimos até essa fase da vida. Após a adolescência, uma íris saudável varia muito pouco pelo resto da vida de um indivíduo, embora uma pequena despigmentação e redução do tamanho médio da abertura da pupila ocorram na velhice.

Um outro aspecto interessante da íris, sob o ponto de vista biométrico, está relacionado com a sua dinâmica de movimentação. Essas alterações ocorrem devido à complexa interação dos músculos da íris (diâmetro da pupila está em constante estado de oscilação). A absorção da luz e outras características fisiológicas podem ser usadas para se evitar possíveis fraudes (ver Apêndice B.2).

Outras características importantes da íris nesse cenário são:

Confiabilidade. Sabe-se que uma íris contém muito mais informação do que uma digital de dedos. Segundo o fabricante LG (*Life's Good*), a probabilidade de se ter duas íris iguais é praticamente uma coisa impossível [w14].

No aeroporto de King Abdul Aziz, na Arábia Saudita, realizou-se um teste em fevereiro 2002 para se verificar a confiabilidade de um sistema baseado em íris. Escolheram-se cerca de 20.000 passageiros cujos dados foram registrados no sistema. Quando se efetuou a identificação dos mesmos, somente 17 tiveram falsa rejeição, sendo que não houve nenhuma falsa aceitação [w15].

Tempo de espera. Para se registrar a amostra inicial, ninguém necessitou de mais de dois minutos. Durante o uso diário do sistema, os tempos de resposta oscilaram entre 1 segundo e 4 segundos, dependendo do dispositivo empregado.

Os sistemas de reconhecimento pessoal são projetados de tal forma que o tempo de identificação não dependa do número de usuários registrados. A varredura de íris atende a esse requisito mesmo em um sistema projetado para trabalhar com base de dados muito grande. Um estudo realizado em 2001 pelo laboratório UK's National Physical Laboratory [w16], [9] afirma na tabela 5 da publicação pertinente que o sistema de reconhecimento por

íris é capaz de reconhecer quase 20 vezes mais amostras por minuto que o seu competidor mais próximo que é a geometria da mão [9].

Prevenção de ataques. A íris é uma das características biométricas mais difíceis de fraudar. Uma íris fora do seu corpo nunca poderia enganar um sistema de identificação. Isso ocorre porque após a morte, a íris perde rapidamente a sua textura impossibilitando a prova de autenticidade. De fato, uma das técnicas empregadas na ciência forense para se determinar a hora da morte de uma pessoa consiste em analisar a íris, por ser uma das partes do corpo que mais rápido se deteriora [w17]. No entanto, uma foto enganaria um sistema que não reconhecesse conjuntamente alguma característica associada à vida.

5.2 Algoritmos de Reconhecimento de Íris

Os algoritmos básicos de reconhecimento de íris variam de acordo com a classificação dada por diferentes autores na literatura. No entanto, em geral os algoritmos contêm uma entrada de dados, um pré-processamento matemático para segmentar a informação, extração de características e uma parte final de comparações para tomar uma decisão (ver Fig. 5.3).

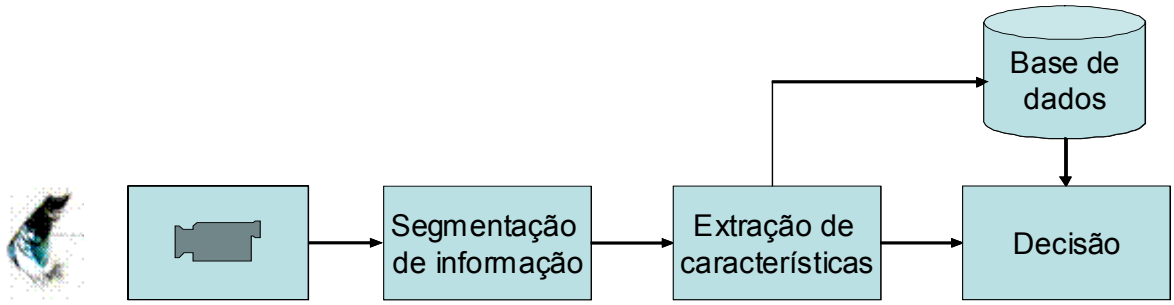


Fig. 5.3 Descrição de um típico sistema de reconhecimento de íris.

A aparência bastante complexa da íris é uma conseqüência das características de sua estrutura, resultando em mais de 400 graus de liberdade [60]. Esse é um parâmetro muito útil para sistemas de reconhecimento, uma vez que expressa quanto os padrões a serem comparados são independentes. Esse valor é três ou quatro vezes maior do que o número de graus de liberdade de sistemas de reconhecimento de impressões digitais [59]. Entretanto, o algoritmo associado ao reconhecimento limita o grau de liberdade.

A seguir descrevem-se brevemente os métodos clássicos de reconhecimento de íris.

5.2.1 Método de J. Daugman

John Daugman foi o pioneiro nessa área, tendo desenvolvido os algoritmos matemáticos que permitiram codificar digitalmente a imagem da íris capturada a partir de um vídeo. Associou-se então a empresa *IriScan, Inc*. que se tornou a principal empresa no mundo a oferecer atualmente esse tipo de serviço. J. Daugman tornou-se uma autoridade reconhecida dentro dessa área de pesquisa [37], [2]. Seus trabalhos são usados como referência na presente pesquisa proposta [61], [52]. O método proposto por Daugman pode ser dividido em quatro procedimentos, ou seja, captura realizada com dispositivos comerciais da empresa *IrisScan* (ver Fig. 5.4), a localização, a normalização, a extração de características e o casamento. A seguir descreve-se cada um desses procedimentos.

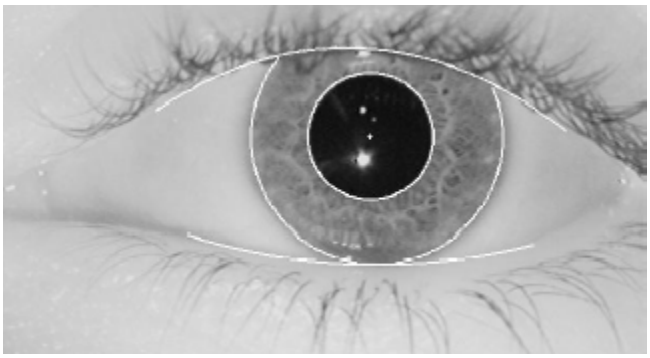


Fig. 5.4 Captura de imagem do olho e localização da íris, método de Daugman [37].

Localização da Íris. O primeiro procedimento é a localização da íris. O autor propõe um operador integro-diferencial para a determinação da fronteira interior da íris com a pupila e da fronteira exterior com a esclerótica. O método está detalhado no Apêndice B.3.2.

Normalização da Imagem. O procedimento de normalização da imagem tem como objetivo a compensação em primeiro lugar das variações de distância entre o indivíduo e a câmera no momento da captura e, em segundo lugar das contrações da pupila devido à iluminação. A normalização transforma o anel que corresponde à pupila na imagem de entrada num retângulo de dimensões fixas. A imagem original ***I(x, y)*** em coordenadas cartesianas é representada agora em um sistema de coordenadas polares na forma ***I(r, q)***, cuja origem está no centro da íris. Essas transformações geométricas são:

$$x(r,\theta) = (1-r)x_p(\theta) - rx_s(\theta) \tag{5.2}$$

$$y(r,\theta) = (1-r)y_p(\theta) - ry_s(\theta) \tag{5.3}$$

Onde $x_p(q)$, $y_p(q)$, $x_s(q)$ e $y_s(q)$ são as coordenadas cartesianas, respectivamente do contorno da pupila e da esclerótica correspondentes ao ângulo θ. Nessas equações r pertence ao intervalo [0,1] e θ pertence ao intervalo [0, 2π]. A transformação resulta em um retângulo conforme se observa na Fig. 5.5

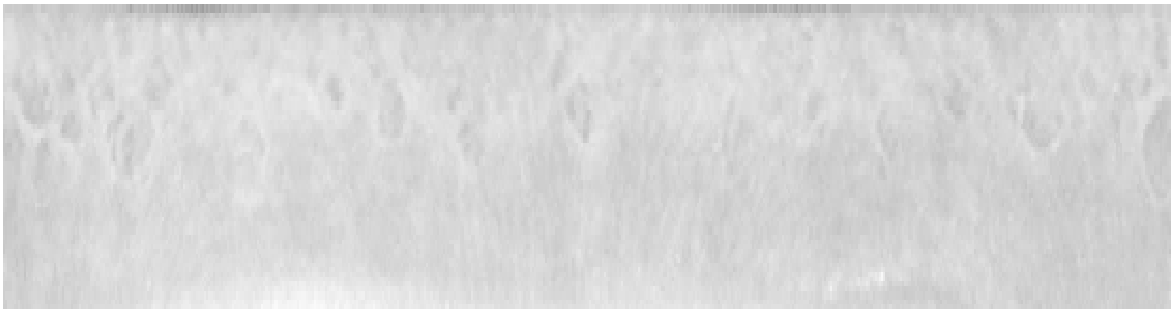


Fig. 5.5 Normalização de Daugman [52].

Extração de características. Para se representar a textura da íris faz-se uso de filtros de Gabor [67], [62] em duas dimensões. Suas propriedades matemáticas foram discutidas por Daugman em 1985 [63]Nesse mesmo trabalho o autor demonstra que os filtros de Gabor 2D em quadratura são notavelmente adequados para se representar texturas. Os filtros de Gabor 2D são definidos assim:

$$H(r,\theta) = e^{-j\omega(\theta_0-\theta)}e^{-(r_0-r)/\alpha^2}e^{-(\theta_0-\theta)/\beta^2} \tag{5.4}$$

Onde, r e θ são coordenadas da imagem normalizada, r_0 e θ definem a posição do filtro, e α e β são as aberturas das gaussianas que compõem o filtro nas direções de r e θ .

Para uma representação da íris, o autor divide a matriz imagem da íris normalizada em blocos de dimensão fixa. Cada bloco é projetado sobre o filtro de Gabor com a forma anterior. Os parâmetros r e θ variam com o inverso de w de modo a produzir um conjunto de filtros centralizados em (r_0, θ_0), posição do centro de cada bloco. Depois dessa decomposição Daugman produz uma representação mais compacta da saída de cada filtro que consiste de dois bits. O primeiro bit dessa representação será 1 ou 0, dependendo da parte real de H(r_0, θ_0) ser positiva ou negativa. Do mesmo modo, o segundo bit será 1 ou 0, dependendo da parte imaginária de $H(r0, \theta_0)$, ser positiva ou negativa. Os valores de $(r0,$

θ_0, α e β), são amostrados de modo a produzir uma representação em 256 bytes chamada de ***iriscode***, que serve de base para o processo de quantização associado a essa passagem (ver Fig. 5.6).

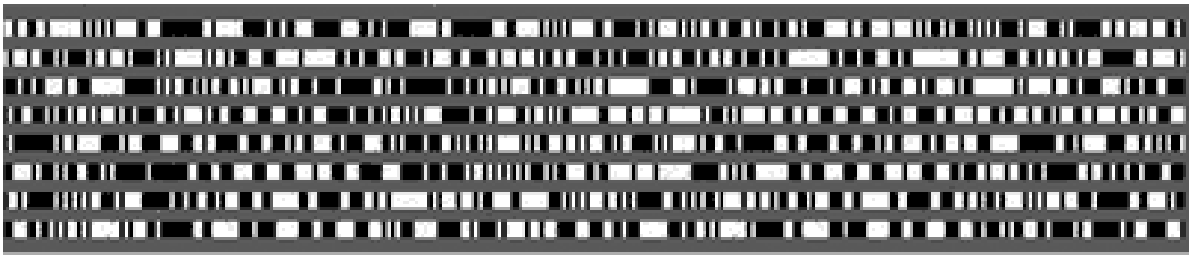


Fig. 5.6 Código de 256 bytes da íris.

Reconhecimento. A similaridade entre duas imagens de íris é determinada pela equação:

$$HD = \frac{1}{2048}\sum_{j=1}^{2048} A_j (XOR) B_j \tag{5.5}$$

A decisão, se duas representações correspondem a uma mesma íris ou a íris distintas é feita com base num limiar determinado empiricamente. O autor sugere ainda um refinamento que leva em conta as áreas afetadas por oclusão que consiste em substituir a métrica do item anterior por uma nova assim definida:

$$HD = \frac{\sum\left[(A_j (XOR) B_j) \cap maskA \cap maskB\right]}{\sum\left[maskA \cap maskB\right]} \tag{5.6}$$

onde *maskA* e *maskB* são máscaras que indicam as áreas não afetadas por oclusão.

Essa medida de similaridade de íris é conhecida como uma distância de Hamming. Quando ocorre um casamento perfeito entre as íris, o valor computado é zero. Para conhecer a probabilidade de as íris comparadas serem diferentes entre si, utilizam-se os dados fornecidos na Fig. 5.7. Essa figura mostra a função de distribuição de probabilidade acumulada (FDPA) experimental da distância de Hamming.

A Fig. 5.7 exibe uma distribuição de probabilidade com média m = 0,499 e desvio padrão de 0,032. Observa-se então que a esperança de uma comparação de íris não relacionadas é 0,5 com um desvio padrão muito pequeno. Isso se deve ao fato de se usar um

cálculo estatístico, uma vez que dado um bit do valor retornado pela codificação, a probabilidade dele ser 0 é a mesma de ser 1, e a comparação entre dois bits não relacionados tem probabilidade média de 50% de chance de ser divergente, isto é, não converge nem para 0 e nem para 1.

Assim na Fig. 5.7, percebe-se que a FDPA para valores de comparação de códigos de íris até 0,4 é muito baixa. Entre 0,4 e 0,5 cresce rapidamente. Valores próximos e acima de 0,5 já são grandes o suficiente para rejeitar com certeza a hipótese de similaridade entre as íris comparadas.

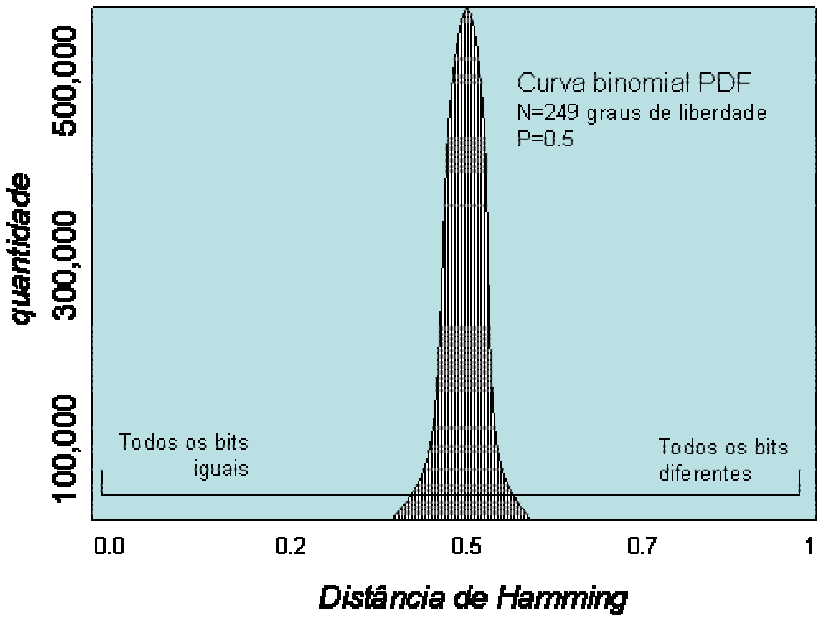


Fig. 5.7 Distribuição da distância de *Hamming* obtida através de 9 milhões de comparações de íris diferentes com média = 0, 499 e desvio padrão 0, 0317 [37].

O algoritmo de Daugman é um dos mais utilizados comercialmente e foi testado exaustivamente conforme descrito em trabalho pertinente [64]. A Tab. 5.1 apresenta a comparação de até 984 milhões de íris sem nenhum falso casamento.

Organização que realizou o teste	Número de comparações	Falso casamento
Sandia Labs, USA (1996)	19 701	0
British Telecom Labs, UK (1997)	222 743	0
Sensar Corp., USA (2000)	499 500	0
Joh.Ensched_e, NL (2000)	19 900	0
EyeTicket, USA (2001)	300 000	0
National Physical Lab, UK (2001)	2,73 milhões	0
J. Daugman, UK (2003)	9,1 milhões	0
Iridian Technologies, USA (2003)	984 milhões	0

Tab. 5.1 Teste do algoritmo de Daugman [64].

5.2.2 Método de W. Boles

O método de Boles representa a estrutura da íris através de uma transformada *wavelet* (Daubechies) diádica contínua [65], [66]. Detalhes dos passos mais importantes são apresentados a seguir.

Localização da Íris. O autor localiza as fronteiras da íris através de um detector de bordas circulares, onde os detalhes não estão documentados no trabalho.

Normalização da Imagem. Uma preocupação importante do sistema de Boles [68]é não onerar demasiadamente o sistema de aquisição de imagens. O método procura ser robusto contra ruído, variações de iluminação e mudanças de distância focal. Usando a imagem com a identificação das fronteiras da íris, 16 círculos concêntricos são traçados.

Representação da íris. O autor utiliza a informação da intensidade de cada pixel presente na imagem como ponto de partida para uma representação da íris. Uma operação semelhante ao método de normalização de Daugman transforma geometricamente cada um dos 16 anéis num vetor com 256 valores. Cada um desses vetores é tratado como amostras de um sinal unidimensional periódico.

Aplica-se a cada sinal 1D uma transformação com *wavelets* diádicas. A aplicação da transformada *wavelet* diádica contínua decompõe o sinal em diferentes níveis de resolução. Como a informação na resolução mais fina é extremamente afetada pelo ruído, somente alguns níveis de baixa resolução foram utilizados, excluindo-se o nível mais alto e os mais baixos, de um total de oito. Experimentalmente, Boles chegou à conclusão que somente o quarto, o quinto e o sexto níveis eram relevantes para a representação de uma íris. O passo seguinte consiste em se calcular a energia entre dois pontos de cruzamento de zero [69] consecutivos no sinal da transformada *wavelet*, usando-se:

$$e_n = \int \psi_{2^j} f(x)dx \tag{5.7}$$

onde e_n é a energia entre os dois pontos de cruzamento, como mostra a Fig. 5.8 .

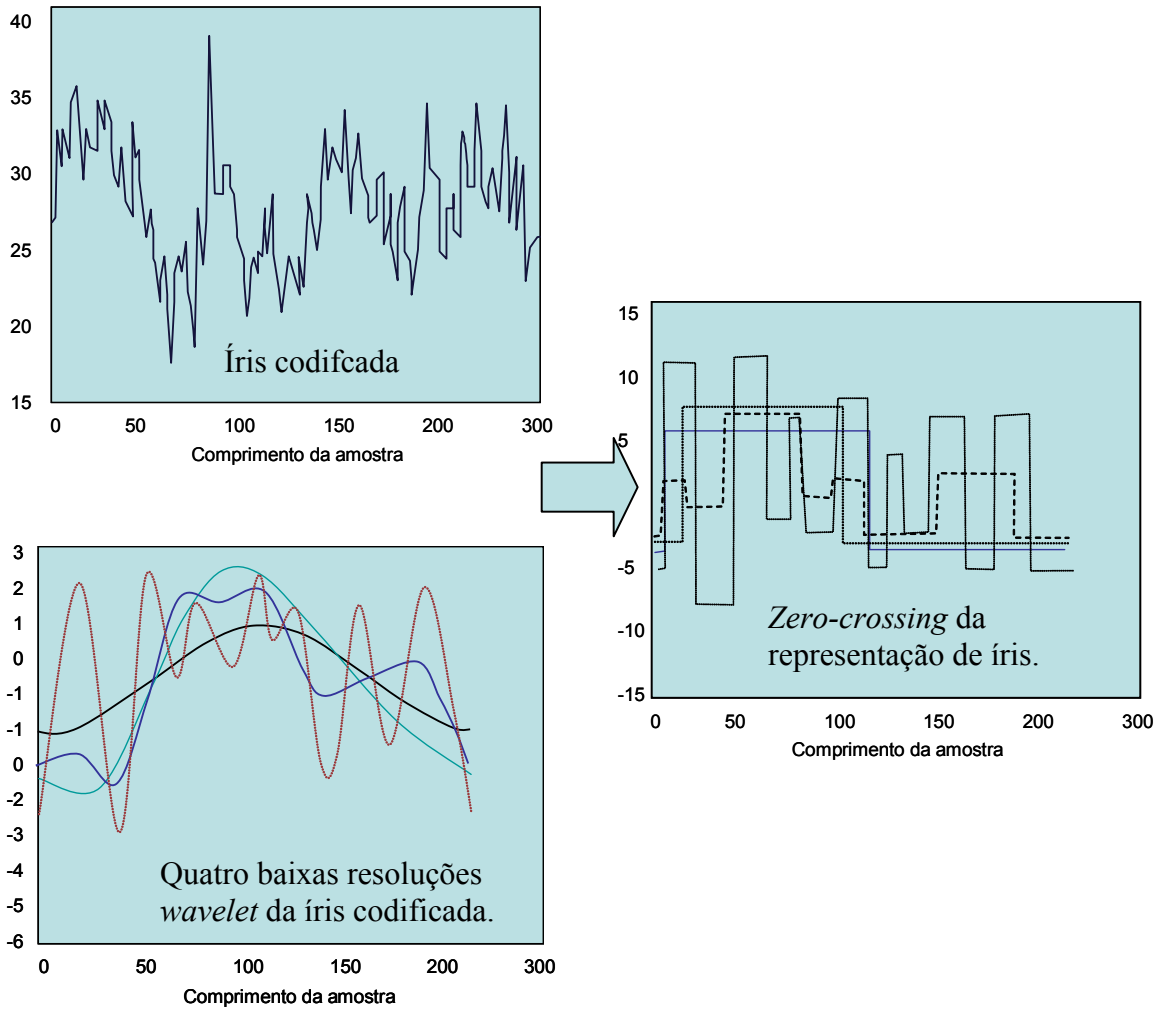


Fig. 5.8 Pontos de cruzamento [68].

A partir dos valores de energia calcula-se então a chamada representação *zero crossing* na forma de um sinal unidimensional que assume entre os pontos consecutivos z_{n-1} e z_n um valor constante Z_n dado por:

$$Z_n = \frac{e_n}{z_n - z_{n-1}} \tag{5.8}$$

Reconhecimento. Para se verificar a similaridade entre duas íris, as representações *zero crossing* de cada uma delas são usadas conforme esclarecido anteriormente. O autor propõe quatro funções para se medir uma similaridade entre os sinais. O melhor desempenho é obtido quando se usa [38]:

$$D_j(f,g) = \min_m \left(1 - \frac{\sum_{n=1}^{N} Z_j f(n) \cdot Z_j g(n+m)}{\left\| Z_j f \right\| \left\| Z_j g \right\|} \right) \tag{5.9}$$

onde *m* está no intervalo *[0, N-1]*. Nessa equação $\boldsymbol{Z_j f(n)}$ e $\boldsymbol{Z_j g(n)}$ denotam o n-ésimo elemento das representações de *zero crossing* no nível *j* de duas íris ***f*** e ***g***. ***N*** é o número de elementos de $\boldsymbol{Z_j f(n)}$ e $\boldsymbol{Z_j g(n)}$ e ***j*** corresponde aos níveis (4, 5 e 6).

5.2.3 Outros Métodos na Literatura

Li Ma propôs um processo baseado na captura de uma seqüência de seis imagens da íris [70]. As imagens são divididas em pequenos blocos, e assim o processo se baseia na localização e reconhecimento desses blocos em cada uma das imagens. Nesse processo, é essencial garantir a qualidade da imagem de entrada, o que se obtém através da análise do espectro em freqüência da imagem. A imagem é segmentada separando-se a área correspondente à íris que é em seguida submetida a uma função de realce. A extração de características considera a informação de textura da região da íris mais significativa, que é a região próxima à pupila e que não é afetada por oclusão. Recorta-se uma região dessa imagem denominada ROI* (*Region of Interest*). Essa região é dividida em blocos, sobre os quais se aplica um filtro de Gabor, do que resulta um vetor de características. A verificação da identidade é realizada usando-se o discriminante de Fisher [70].

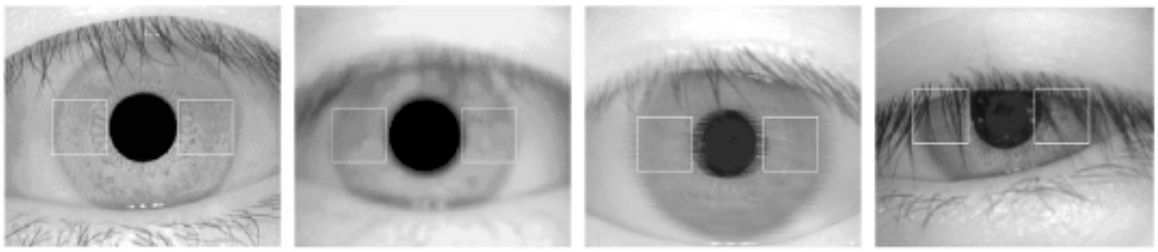


Fig. 5.9 Regiões de menores oclusões [70].

Posteriormente, Li Ma publicou a descrição de outro sistema eficiente de reconhecimento de íris. O sistema baseia-se na geração de sinais em 1D, utilizando um esquema semelhante ao de Boles. O objetivo foi de tornar o sistema mais eficiente. Utilizaram-se as variações locais do sinal, caracterizando-se esse sinal em somente dois níveis de resolução. Os resultados obtidos foram bons em termos de precisão com uma

diminuição de complexidade [71].

Sanchez-Avila e Sanchez-Reillo deram continuidade ao trabalho de Boles desenvolvendo um sistema que utiliza a representação *zero-crossing* da transformada *wavelet* para se construir *templates* da íris. A inovação em relação ao trabalho de Boles foi a introdução de técnicas baseadas em métricas de distância como a Euclidiana e a distância de Hamming para os processos de verificação e decisão [72], [73].

C. Tissel, apresentou uma modificação no algoritmo de Daugman com duas grandes diferenças: a primeira relacionada à localização da íris e a segunda na etapa de extração de características. O algoritmo de Tissel aplica a transformada de Hough para estimar o centro da pupila e adota um operador semelhante ao proposto por Daugman para determinar as fronteiras da íris. Para as tarefas de extração de características e representação, a transformada de Hilbert 2D é usada, construindo-se a partir daí uma imagem denominada analítica, a qual é codificada em um vetor que armazena uma informação de freqüência e fase [74].

S. Noh propôs um novo método para se representar as características da íris, baseado em M-ICA (*Multiresolution Independent Component Analysis*). ICA é um algoritmo não supervisionado usado para redução de dimensionalidade que faz uso de estatísticas de alta ordem e o M-ICA é um novo método para extração de características, introduzido pelos autores. O autor apresentou comparações com técnicas baseadas em *wavelets* de Gabor, Haar e Daubechies juntamente com o método proposto. O discriminante de Fisher foi adotado como ferramenta de classificação [75].

5.3 Sistemas de Reconhecimento de Íris: Área Comercial

Um dos maiores difusores da tecnologia de reconhecimento de íris é o IriScan, detendo patentes exclusivas em mais de 20 países, sobre os conceitos de reconhecimento de íris, originado por Leonard Flom e Aran Safir e usando o *software* de Daugmam. Atualmente, é utilizado em diversas empresas e departamentos.

Exemplos: *US House of Representatives*, *US Department of Treasury*, *Bank United (Texas), AK Bank (Turquia), British Telecommunication, Brussels Bank, KPN Telecom (Holanda), Hewlett Packard, Lake Contris Sheriff's Office, Olimpic Memorial Hospital*, etc.

No intuito de embarcar sua tecnologia em sistemas maiores, o IriScan associou-se a outros vendedores, como Sensar e LG.

J. Daugman, um dos criadores do *software* mais utilizado na literatura apresenta no site da internet [37] algumas das empresas que utilizam o método de reconhecimento de íris por ele criado.

Patentes

As patentes que servem como base para os produtos comerciais basicamente são:

Leonard Flom, Aran Safir: *Iris recognition system. International patent* WO8605018A1, 28 *August* 1986 *and US Patent* 4641349 *issued* 2/3/1987.

John Daugman: *Biometric personal identification system based on iris analysis*. U.S. *Patent* No. 5,291,560, 1 *March* 1994.

5.4 Aplicações

As aplicações dessa biometria baseada em íris são bem difundidas em ambientes de alta segurança e estão se expandindo no mundo. Por exemplo:

- Fronteiras de países estão utilizando atualmente (2006), sistemas de reconhecimento de íris em passagens alfandegárias do Canadá, Holanda, Singapura e nos Emirados Árabes Unidos.
- Aeroportos, como o JFK (John Fitzgerald Kennedy) nos EEUU ou Narita no Japão, já estão equipados em maior ou menor escala com sistemas de reconhecimento baseados em íris.
- No centro de dados da British Telecom, um dos mais prestigiosos do setor de telecomunicações com capacidade para 12.000 servidores e 300 empregados, decidiu-se implantar um sistema de identificação baseado em íris, depois do episódio de atentado nos USA.
- Em Hospitais: O acesso aos dados médicos dos pacientes somente pode ser realizado depois de uma identificação pelo sistema de reconhecimento de íris, em alguns hospitais de Washington, DC, Pennsylvania e Alabama.
- Campos de refugiados: Em outubro de 2002, a Alta Comissão para os Refugiados das Nações Unidas começou a usar o reconhecimento de íris para registrar refugiados afegãos em Peshawar, Paquistão. Na repatriação, cada refugiado recebeu pacotes de ajuda sendo que o sistema de identificação por íris foi usado a fim de se minimizar as fraudes.
- Penitenciárias como as de *Lancaster* usam um sistema de identificação para receber visitas que são previamente verificadas biometricamente para ter o acesso ao encarcerado. Isso ocorre desde maio de 2001.
- Caixas automáticos. No Reino Unido há vários anos estão em teste caixas automáticos capazes de reconhecer a íris dos usuários.
- CHILD Project: O projeto (*Children's Identification and Location Database*) pertence ao *Nation's Missing Children Organization* (NMCO), uma associação

estadunidense que luta contra o problema das crianças desaparecidas. O projeto está implantado ou em processo de implantação, em boa parte dos estados dos EEUU, e usa a íris como método de identificação biométrica [w18].

- Verificação da identidade de uma pessoa da qual se tem uma fotografia. Como exemplo, tem-se o caso da famosa mulher afegã que aparece em uma reportagem da *National Geographic*. Ela foi reconhecida 18 anos mais tarde, sendo que na identificação aplicou-se o algoritmo *iriscode* de John Daugman.

Brasil:

- A Politec é a maior empresa privada de serviços de tecnologia da informação do Brasil. Tem parceria com a Iridian Technologies onde se pesquisa e desenvolve aplicações biométricas baseadas em íris [w19].
- Pesquisas estão também sendo feitas no INPE (Instituto Nacional de Pesquisas Espaciais)- UBC - Universidade Braz Cubas - Laboratório de Neurocomputação e Computação Emergente [w20].
- Alguns hospitais, clubes e hotéis no Brasil já estão usando a tecnologia biométrica sendo que o reconhecimento de íris é também utilizado pela Telefônica [w1].

Capítulo 6

Reconhecimento de Íris: Proposta e Recomendações

Neste capítulo apresenta-se uma proposta a fim de se melhorar a eficiência de um sistema de reconhecimento de íris.

No tocante à captura de dados realizada por dispositivos físicos apresentou-se apenas um estudo atualizado, sendo recomendável um sistema de desligamento automático baseado em histograma.

No bloco de *liveness*, os estudos realizados chegam à conclusão de que esse problema é complexo, sendo que para cada tipo de ataque pode-se providenciar um de contra ataque. Assim, a recomendação é obter informações sobre os tipos atuais de ataque, contra ataque e métodos de *liveness* que possam ser aplicados em cada condição específica.

A etapa de localização constitui o foco da presente pesquisa. Apresenta-se uma proposta que torna o sistema mais rápido em comparação com o método clássico. O método clássico utiliza uma matriz acumuladora enquanto que o proposto usa um conjunto de variáveis, resultando em uma diminuição na quantidade de memória utilizada e no tempo de processamento. O esquema de localização usa parametrização, segmentando-se a informação relevante da íris. Concomitantemente usa-se um esquema de concentricidade de íris e pupila transformando a normalização em um módulo simples. Os resultados experimentais quando se substitui essa proposta de localização no modelo de Masek [11], [12] são mostrados no próximo capítulo. O desempenho do sistema é medido em termos de eficiência no tempo, mantendo-se a exatidão [82].

A simulação do sistema baseia-se no algoritmo de Daugman [11]. Esse algoritmo é um dos mais extensamente testados e aplicados atualmente. A utilização de transformadas possibilita uma maior rapidez de processamento. Dessa forma, melhora-se o desempenho desse tipo de reconhecimento de íris. Especificamente, utiliza-se a transformada de

wavelets.

O casamento é obtido por uma operação XOR, o que é feito na maioria das principais implementações relatadas na literatura. Como se trata de um modelo binário, esse tipo de operação é muito rápido e os resultados são satisfatórios.

Assim, o sistema descrito é apresentado na Fig. 6.1.

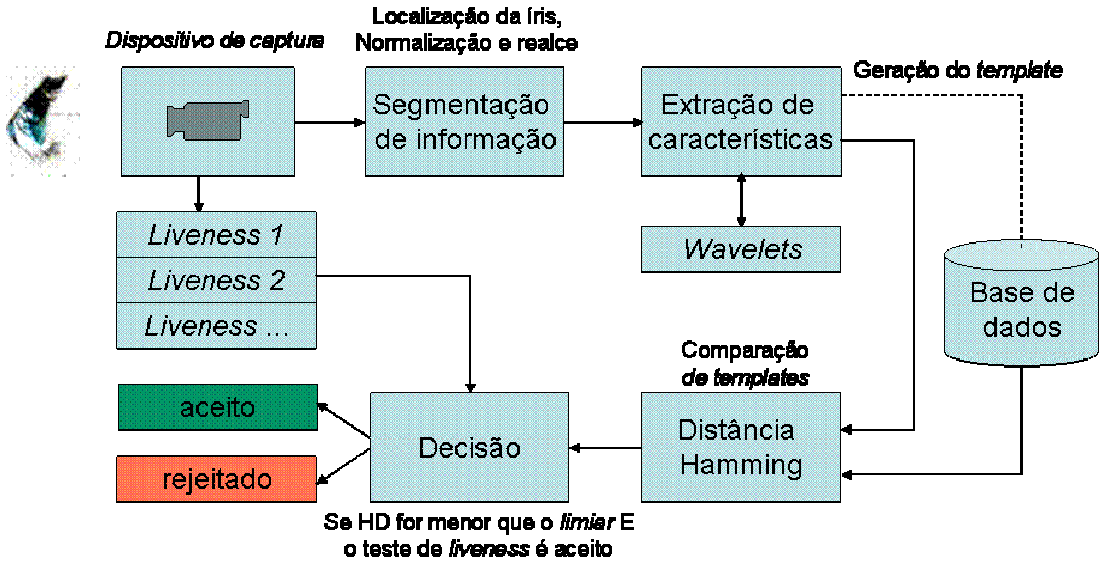


Fig. 6.1 Sistema de reconhecimento de íris estudado.

6.1 Captura de Dados

A captura de dados e o *Liveness* constituem os blocos iniciais do processo de reconhecimento.

A captura de dados é feita por algum dispositivo, normalmente uma câmera digital. Após a obtenção da imagem digital, aplica-se um teste de segurança contra fraudes chamado de *liveness*. No Apêndice B, apresentam-se mais detalhes sobre esses blocos iniciais.

Nesta sessão realiza-se um estudo inicial sobre os métodos utilizados, bem como sobre algumas recomendações para um projeto de sistema.

Inicialmente, aborda-se o tema sobre captura de dados. Os esquemas de Daugman foram testados e funcionam de acordo com as publicações. No entanto, além da forma de se capturar a imagem, devem-se levar em conta outros fatores. De fato, o objetivo da captura de dados é a obtenção de uma imagem que sirva para reconhecimento. Assim, qualquer que seja o dispositivo usado, o resultado deverá fornecer os parâmetros de imagens adequados para o reconhecimento. Dessa forma, se dois ou mais equipamentos permitem a obtenção

de parâmetros com a mesma definição, claridade e contraste das imagens para a composição de uma base de dados, então não haverá necessidade de se ajustar o algoritmo. O ideal é tentar imitar as formas finais das imagens obtidas, ajustando-se os equipamentos. Outro aspecto importante na captura de dados para um algoritmo trabalhando em tempo real é a eficiência mesmo que se use um computador convencional. Em geral, os equipamentos são dedicados e, portanto normalmente são mais rápidos do que os computadores. De fato, se o equipamento está constantemente ligado, o computador estará trabalhando continuamente dados não importantes. Para se contornar esse problema faz-se uma análise de histograma a fim de se caracterizar a presença de um olho. Dessa forma, pode-se iniciar o processo de reconhecimento somente depois da aquisição de uma imagem correspondente a um olho. Isso é simples de ser realizado, aplicando-se limiares ao histograma e detectando-se um pico que represente a pupila (ver Fig. B.4 do Apêndice B).

Outro aspecto que pode ser considerado é a detecção de *liveness*. Quando esse bloco é inserido no passo inicial, o impostor terá acesso no máximo, até a entrada da câmera. Nesse caso, o usuário inicia o ataque possivelmente com uma imagem ou uma lente de contato. De acordo com o dispositivo usado, pode-se propor uma metodologia de contra ataque. Por exemplo:

Coletam-se N imagens por segundo (frame). Nesse caso, considera-se como sendo uma característica da íris a variação de tamanho (contração e dilatação) da pupila. Providenciam-se mudanças curtas de luminância que afetem a pupila durante um intervalo de tempo Δt e analisam-se M imagens. Comparam-se as pupilas de acordo com essas mudanças de luminância. Por exemplo, se a luminância foi aumentada então se espera que o tamanho da pupila tenha diminuido gradativamente nas M imagens. Se o tempo for curto (menor do que um segundo), a chance do impostor ter sucesso diminui.

Um outro fenômeno que pode ser explorado é o grau de reflexão do olho. A quantidade de luz refletida por uma membrana viva é muito irregular, por ser esferoidal e porque ela é mais absorvente do que uma imagem impressa (ou lente de contato). Assim, usando-se um detector de nível de absorção de luminância podem-se propor soluções para o problema de íris impostor.

Para cada tipo de ataque conhecido deve-se aplicar um contra ataque. O processo de avaliação deve levar em conta o tipo de aplicação a fim de se verificar a necessidade de inserção ou não do bloco de *liveness* de acordo com o ambiente analisado.

6.2 Localização

Têm-se conseguido muitas melhoras no reconhecimento de íris, mas alguns problemas não podem ser ignorados. Os sistemas reais, em condições variantes requerem muita

robustez. No entanto, também é necessário adicionar rapidez, dado que são capturadas várias imagens por segundo. Além disso, o usuário tem pouca tolerância a longos tempos de processamento. Os custos de localização estão próximos da média total do processo [71] e a localização da íris é importante para a seqüência de processamento. A localização é crucial para o melhor desempenho em relação ao tempo e à precisão do sistema de reconhecimento [82]. Em diversos trabalhos, um dos problemas que não foi resolvido é a falta de exatidão na localização. Sugere-se esse tema como pesquisa futura [84], [12]. Nesse caso, simplesmente não se utilizam as amostras erradas nessa etapa (ver Fig. 6.2).

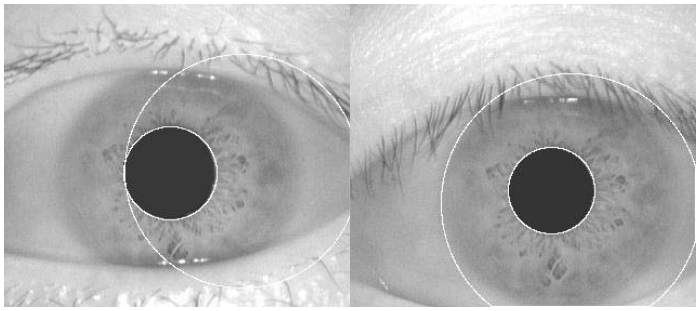


Fig. 6.2 Erros acentuados na localização com a transformada de Hough (imagem 52).

Um requisito importante a ser satisfeito é a necessidade de balanceamento entre o tempo de localização e o tempo necessário para obtenção de uma exatidão aceitável. A descrição do método clássico e de outros métodos atuais é apresentada no Apêndice B.

6.2.1 Análise da Textura de Íris

As imagens utilizadas nesta dissertação estão na cor cinza com diferentes níveis de intensidade. Os valores variam de 1 a 256, sendo essa escala denominada escala de cinza (*greyscale*). A íris está situada perto da pupila. Ela tem características radiais e angulares. Isso forma uma textura, dado que essas características ou padrões resultam em mudanças na intensidade da imagem formada. A pupila tem formato mais semelhante ao de um círculo do que a íris. As características angulares estão mais presentes próximos à pupila enquanto que as radiais se iniciam na pupila, dado que estas últimas correspondem aos músculos responsáveis pelos movimentos de contração [78]. Isso é mostrado na Fig. 5.2. Além disso, na Fig. 6.3 observa-se que a captura de dados de textura concêntrica contém a informação mais relevante da íris. A maioria das características é concêntrica, mesmo quando a íris não é concêntrica [85], [86], [87], [w21].

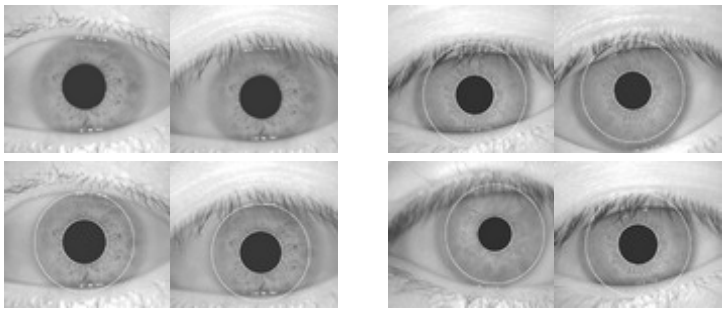


Fig. 6.3 Concentricidade da textura de íris com a pupila (Casia v.1).

A textura da íris pode ser utilizada para reconhecimento [70],[71]. No presente trabalho utiliza-se a transformada de *wavelets*. Essa transformada faz uma análise de textura e gera um *template* baseado nessas características. Quando se tem um algoritmo baseado em textura, a informação relevante é a mesma. Dessa forma, torna-se mais importante segmentar a textura do que localizar a íris como tal.

6.2.2 Proposta para a Localização de Íris

A presente proposta para a localização é voltada para se segmentar a informação de textura da íris. O modelo de reconhecimento utiliza *wavelets* a fim de caracterizar texturas. Isso é baseado no cálculo aproximado da pupila, através da intensidade mínima das projeções vertical e horizontal. Encontra-se o raio da pupila de forma iterativa utilizando-se as mudanças de intensidades (0,1). Refina-se a posição do centro e acha-se o raio da íris analisando-se somente uma região centrada (X_p, Y_p). Substitui-se a detecção de bordas por um filtro que mostre uma variação binária simples nos dois eixos para se encontrar a pupila. A procura é feita na linha de menor intensidade para cada eixo. Usa-se uma detecção do raio da íris similar à anterior, mas em um só eixo. O algoritmo proposto tem a vantagem de ser rápido e de menor complexidade, porém é sensível a erros devido às obstruções que afetam a intensidade de outras regiões. Aplicando-se ruído gaussiano na localização ter-se-á a mesma resposta, isso porque se usa a média da intensidade em uma linha. Aplica-se assim nesses casos o ruído gaussiano, e assume-se a resposta como sendo válida. A seguir detalha-se cada parte do algoritmo proposto.

Localização do centro aproximado da pupila

A primeira localização do centro da pupila é conseguida através da característica que é mais uniforme e de menor intensidade na imagem do olho. Então se aplica o seguinte algoritmo:

- Passar um filtro mediano, que garanta uma suavização suficiente para diminuir o ruído e diferenciar as regiões de alta e baixa intensidade. Esse tipo de filtro é utilizado para

ajudar a segmentar a textura e a detecção de bordas de células. No caso da íris, ocorre um fenômeno semelhante ao uso de um microscópio. Nesse último caso, o limite da célula com o fundo é também pouco diferenciado. O uso do filtro provê resultados que são melhores do que os obtidos com os operadores tradicionais de Sobel, Prewitts, Roberts, e o método Laplaciano [98].

- Converter os dados da imagem para o sistema binário. Utiliza-se um limiar que garanta uma intensidade da pupila diferente da intensidade da íris. O algoritmo tem como limiar experimental 26% da máxima intensidade possível. Isso depende muito dos parâmetros de obtenção da imagem. Com o aumento do contraste, o limiar aumenta. Deve-se achar (X_p, Y_p) aplicando-se [71]:

$$X_p = \arg\min_x \left(\sum_y I(x,y) \right) \tag{6.1}$$

$$Y_p = \arg\min_y \left(\sum_x I(x,y) \right) \tag{6.2}$$

onde (X_p, Y_p) é o centro aproximado da pupila.

Raio da pupila

Tendo-se (X_p, Y_p) aproximados, deve-se:

- Percorrer *pixel* a *pixel* desde o centro (X_p, Y_p) até se chegar a uma região de mudança de intensidade $I(x,y) = 0$ (cor preta) para uma $I(x,y) = 1$ (cor branca). Nos sentidos esquerdo e direito para o eixo x, acham-se respectivamente, x_l e x_r. E nos sentidos acima e abaixo para o eixo y, acham-se respectivamente, y_u e y_d.
- Dados x_l, x_r, y_u e y_d estimar o raio da pupila, aplicando-se as seguintes equações:

$$R_p^x = \frac{\left|X_p - x_l\right| + \left|X_p - x_r\right|}{2} \tag{6.3}$$

$$R_p^y = \frac{\left|Y_p - y_u\right| + \left|Y_p - y_d\right|}{2} \tag{6.4}$$

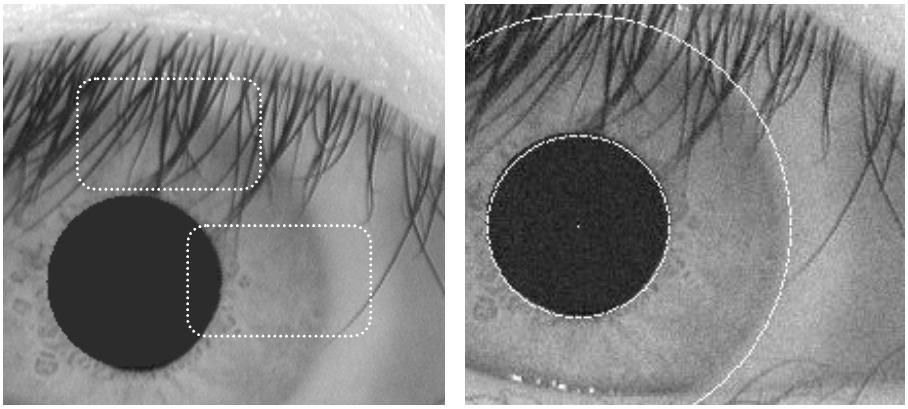
$$R_p = R_p^x \approx R_p^y \tag{6.5}$$

onde R_p, R_p^x e R_p^y são as aproximações do raio da pupila nos dois eixos. R_p assume o valor de R_p^x dado que ele sofre menos obstruções dos cílios e das pálpebras, e é somente utilizado para comparar se o resultado está coerente.

Localizar o centro real da pupila

Agora com os dados aproximados de (X_p, Y_p) e R_p, pode-se encontrar o centro real da pupila.

- Achar o erro $\varepsilon = \left| R_p^x - R_p^y \right|$, se ele for maior do que o máximo erro permitido. Então, aplicar ruído gaussiano à imagem original. Iniciar de novo o algoritmo tendo a nova imagem de entrada. Uma imagem com ruído gaussiano ou sem ele, terá um resultado conforme mostrado na Fig. 6.4. No entanto, para os casos com muitas obstruções verticais de baixa intensidade como se observa na Fig. 6.4 (a), o algoritmo baseia sua procura em informações de baixas intensidades o que nesse caso é indesejável. Isso porque tal procura resultará em linhas contínuas verticais que poderiam ser confundidas com o círculo limite da pupila. A inserção do ruído gaussiano minimiza o efeito dessas continuidades.



(a) (b)

Fig. 6.4 (a) Íris com obstrução vertical dos cílios, e outra região com pouca incidência deles; (b) Localização de íris aplicando-se ruído gaussiano.

- Então, reinicia-se o algoritmo, mas agora com a informação dos raios R_p^x e R_p^y. Os efeitos interferentes dos cílios normalmente ocorrem na vertical. Logo, o raio R_p^x é o raio da pupila R_p final válido (para satisfazer a condição de um erro ε). Nos testes, apenas uma das 108 classes da base de dados CASIA [13] necessitou realmente do tratamento de ruído como na Fig. 6.4 (b). Assim, esse passo insere robustez ao algoritmo.
- Calcular as coordenadas do centro:

$$(X_p, Y_p) = \left(\frac{x_r + x_l}{2}, \frac{y_u + y_d}{2} \right) \tag{6.6}$$

Nesse algoritmo (X_p, Y_p) é considerado válido dessa etapa em diante.

Raio da íris

O algoritmo processará somente a região da imagem que contém a menor quantidade de obstruções. No caso de uma imagem pertinente a um olho, essas regiões de menor

obstrução são as regiões que ficam ao lado do centro da pupila. Essas regiões de interesse (ROI*) podem ser utilizadas para o todo o processo [70]. Na Fig. 6.4.(a) tem-se um exemplo onde se percebe com clareza que os cílios ou as pálpebras dificilmente chegam a cobrir a informação da íris. Assim, deve-se:

- Compor uma janela centrada em (X_p, Y_p), de comprimento e largura dadas por:

$$[M \times N] = [2(R_p + eRi_{\max}) \times \text{height}] \tag{6.7}$$

onde $eRi_{\max}$, é a variação máxima do raio da íris que ocorre em relação ao centro. Depende de muitos fatores relacionados com a forma de aquisição da imagem, tais como a iluminação, distância da câmera, porcentagem do olho na imagem, etc. Nos testes realizados, usa-se a base de dados CASIA [13], na qual esses parâmetros têm valores constantes em todas as imagens. A variável *height* que corresponde à altura tem valor que depende da base de dados. Um valor menor levará a um menor tempo de processamento, porém, haverá maior probabilidade de que as obstruções inviabilizem o processo. O valor para essa variável é empírico, tendo o valor de seis pontos o melhor comportamento. Aplicou-se o filtro mediano nessa janela para passar a informação relevante da textura para baixa intensidade a fim de suavizar as fronteiras de textura da íris e desprezar a região externa se for necessário.

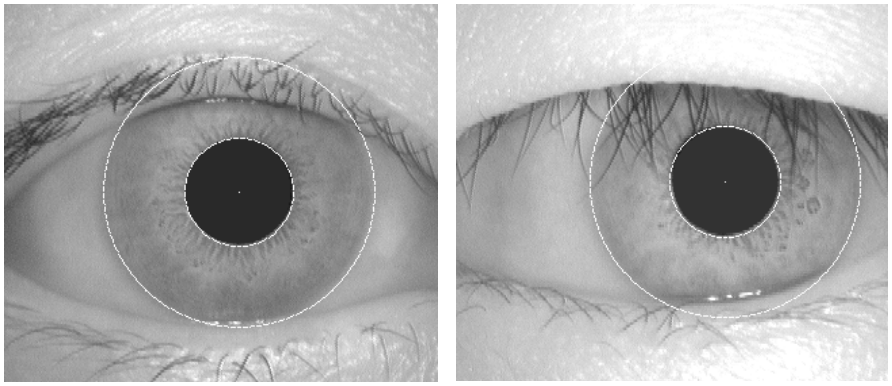
- Passo de busca: procurar desde um canto da janela até encontrar um ponto x_l, x_r de baixa intensidade no eixo horizontal, indo para o lado esquerdo e para o direito. Esses são os limites aproximados da íris.

$$R_i = \frac{|X_p - x_l| + |X_p - x_r|}{2} \tag{6.8}$$

- Obter o centro da íris (X_i, Y_i)

$$X_i = |x_r + x_l|/2 \tag{6.9}$$

Mesmo que a exatidão de localização seja menor, os dados perdidos não são tão relevantes para o cálculo final. Isso porque a maior informação da íris está na região mais próxima da pupila (segmentação). Note-se que o filtro mediano retira apenas a informação no limite exterior da íris que apresenta textura quase nula (ver Fig. 6.3).



(a) (b)

Fig. 6.5 Localização da íris proposta: centros e raios de pupila e íris.

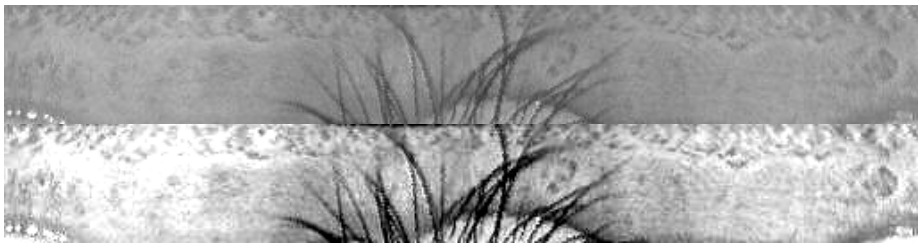
A localização será finalizada somente depois que os resultados em cada passada do algoritmo forem iguais (menores do que o erro ε). Na Fig. 6.5 observa-se o resultado com uma iteração. No caso (a) quase sem obstruções e no caso (b) com obstruções da pálpebra e dos cílios.

6.3 Normalização

A aquisição de uma imagem real no meio ambiente dificilmente é perfeita. Os erros inseridos são devidos às muitas variáveis envolvidas, tais como os diferentes tamanhos das íris, as variações de iluminação, bem como de outros fatores que afetam a imagem (ver Tab. 3.6), incluindo-se as reações naturais da pupila. Para se obter uma informação confiável da íris deve-se localizar a íris e uniformizar esses dados para que os algoritmos computacionais de reconhecimento possam realizar a análise.

O processo de normalização é responsável por gerar imagens com dimensões constantes. Assim, imagens da mesma íris capturadas sob condições diferentes terão suas características em uma mesma localização espacial. Neste trabalho foi simulada a técnica de normalização proposta por John Daugman [52], [61], [65]-[67] implementada por L, Masek [11], [12].

O conteúdo circular em uma imagem padrão de íris pode ser representado em uma imagem retangular. Assim, aplica-se uma transformação para se passar de uma faixa circular para um retângulo (ver Fig. 6.6).



(a)

(b)

Fig. 6.6 (a) Íris em formato (64x512) normalizado em um retângulo; (b) Realçando a imagem aplicando-se maior contraste.

Ao normalizar uma imagem devem-se ter parâmetros fixos a fim de simplificar os passos subseqüentes de processamento sem reduzir os dados relevantes nem causar distorções [2], [70]. Tem-se:

$$I_n(X,Y) = I_o(x,y) \tag{6.10}$$

$$x = x_p(\theta) + (x_i(\theta) - x_p(\theta))\frac{Y}{M} \tag{6.11}$$

$$y = y_p(\theta) + (y_i(\theta) - y_p(\theta))\frac{Y}{M} \tag{6.12}$$

$$\theta = 2\pi X / N \tag{6.13}$$

onde I_n é a nova imagem de $M \times N$ (64 x 512).

A imagem normalizada conserva as características principais da textura como observado na Fig. 6.6 (a), mas a íris é de baixo contraste e as informações relevantes são as mudanças de textura. Por essa razão, o tratamento da imagem na Fig. 6.6 (a), consiste em se realçar as regiões que contém os dados. Com localização precisa e normalização sem deformação, as informações de textura estão prontas para posteriores tarefas de reconhecimento, porém, reduzindo-se os dados.

Finalmente, o processo de normalização usado em conjunto com o método de localização proposto (de circunferências concêntricas) é mais simples e funciona adequadamente. Têm-se também esquemas elípticos e outros tipos de forma [92] que requerem maior trabalho computacional, mas que não são estudados neste trabalho.

6.4 Codificação e Casamento

A codificação está baseada na transformada de *wavelets*, utilizando-se o esquema de Daugman. A extração de características é feita pelos filtros de Gabor (ver Cap. 5.2.1), utilizando-se uma modulação própria do autor [65].

6.4.1 *Wavelets*

No processamento de sinais, a transformada de Fourier tem como objetivo transformar um sinal do domínio de espaço para o domínio de freqüência , [104]. As *wavelets*, diferentemente da transformada de Fourier, têm como base uma função de duração limitada, isto é, de suporte compacto. Isso resulta em uma propriedade importante, em que seu domínio para valores diferentes de zero tem uma extensão finita e para valores iguais a zero no restante (extensão infinita). Isso torna interessante a utilização das *wavelets* no caso específico da análise de imagens, pois as mudanças de regiões ou bordas podem ser detectadas mais facilmente.

A definição de uma transformada de *wavelets* será descrito brevemente baseado na pesquisa e notação utilizada em [99], [108]. Considerando um sinal continuo f(t), a transformada de *wavelets* é dada por:

$$TWC(a,b) = \int f(t)\psi_{a,b}(t)dt \tag{6.15}$$

Nessa equação, os parâmetros *a* e *b* variam continuamente em **R**, sendo que as funções $\psi_{a,b}$ são denominadas *wavelets* e definidas da seguinte forma:

$$\psi_{a,b}(t) = (\frac{1}{\sqrt{a}}).\psi(\frac{t-b}{a}) \tag{6.16}$$

A transformada de *wavelets* para sinais discretos é definida como:

$$TWD(a,b) = a_0^{-m/2} \int f(t)\psi(a_0^{-m}t - nb_0) \tag{6.17}$$

Pode-se ver claramente que o comportamento dessa função está baseado em dilatações e translações a partir de uma *wavelet* mãe ψ sendo que $m, n \in \mathbf{Z}$ e a_0, b_0 são constantes. Em ambos os casos, essa *wavelet* mãe, deve satisfazer a propriedade:

$$\int \psi(t)dt = 0 \tag{6.18}$$

Observando a equação (6.15), percebe-se que a transformada de *wavelets* depende de dois parâmetros *a* e *b*, que correspondem às informações de escala e tempo, respectivamente.

Obter os coeficientes de *wavelets* em cada escala possível requer uma grande quantidade de cálculo, tornando muito tedioso o trabalho (transformada contínua de *wavelets*). Devido a esse fato, a transformada discreta de *wavelets* escolhe um subconjunto de escalas e

locações sobre os quais se realizam os cálculos.

Segundo Daubechies dentro da transformada discreta de *wavelets* distinguem-se duas abordagens: sistemas redundantes discretos (*frames*) e ortonormal (e outras) bases de *wavelets*. A segunda abordagem considera a estratégia de análise de multiresolução, desenvolvida por Mallat [105], [106].

6.4.2 Wavelets de *Gabor*

A transformada *wavelets* de Gabor originalmente proposta como funções Gabor, tem conseguido resultados promissores quando utilizadas em aplicações de reconhecimento de textura e objetos. As *wavelets* de Gabor são especialmente apropriadas para representação de características locais pelo fato de apresentar as seguintes propriedades: são boas *wavelets* localizadas no tempo e na freqüência e também porque elas contêm um maior número de parâmetros.

Funções *Gabor* e *Wavelets*

Uma função bi-dimensional de Gabor $\psi(x, y)$, usada como a *wavelet* mãe, é definida como:

$$\psi(x,y) = \left(\frac{1}{2\pi\sigma_x\sigma_y}\right)\exp\left[-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\right)+2\pi jWx\right] \tag{6.19}$$

onde σ_x e σ_y são os desvios padrões de $\psi(x, y)$ ao longo dos eixos x e y, respectivamente. A constante W determina o comprimento de banda de freqüência dos filtros.

As funções de Gabor formam um conjunto de bases completo, embora sejam não ortogonais.

As *wavelets* de Gabor podem ser interpretadas como um conjunto de funções Gabor com distintos centros de freqüência e orientações. O tamanho ou o comprimento de banda das *wavelets* de Gabor é também controlado por θ. Pelo fato das *wavelets* Gabor serem simétricas, deve-se especificar apenas o valor de θ para se montar um espaço uniformemente amostrado em $[0, \pi]$. Dessa forma, o conceito de localização das *wavelets* de Gabor estendeu-se para o tempo, freqüência e orientação. A não ortogonalidade das *wavelets* Gabor implica que existe uma informação redundante nas imagens filtradas. É possível diminuir a informação redundante.

6.4.3 Distância de *Hamming*

Uma distância de Hamming é uma medida quantitativa da variação entre bits e entre *templates*. Essa medida é obtida através da comparação bit a bit dos *templates* seguida do cálculo da razão entre a quantidade de bits que não se correlacionam e a quantidade total de comparações entre bits. A distância euclideana é aquela entre dois pontos enquanto que a de *Hamming* é simplesmente a somatória de 1's ou 0's. Essa medida é utilizada com sucesso em várias aplicações de processamento de sinais. Por exemplo, pode ser usado na implementação de correlatores baseados na distância de *Hamming* generalizada, a fim de se recuperar o sincronismo no tempo de um sinal OFDM (*Orthogonal Frequency Division Multiplexing*) [w22].

Para o casamento, uma distância de Hamming é utilizada como uma métrica em reconhecimento, bit a bit. A distância de Hamming trabalha com máscaras onde os bits não significativos são omitidos e somente são utilizados os bits úteis entre dois *templates* de íris (ver Sec. 5.2.1). A segmentação utilizada para criar essa máscara e tirar esses bits é feita pela TH para linhas [11], [12].

Teoricamente, dois *templates* de íris gerados a partir da mesma íris deveriam ter a distância de Hamming igual a zero, no entanto na prática isso não acontece, devido a uma normalização imperfeita, aos ruídos não detectados ou alguma variação na comparação de dois *templates* intraclasse.

6.5 Resultados e Simulações

A ferramenta utilizada para os experimentos foi desenvolvida no laboratório de comunicações visuais (LCV/Decom/Feec/Unicamp), que está equipado com um computador Pentium IV 3.2 GHz, 256Mb RAM, que roda o Matlab 7.1, em ambiente operacional Windows 2000.

Para se avaliar o desempenho do método proposto, foi utilizada a base de dados *CASIA Íris Database*, que contêm 756 imagens (320x280 pixels) de íris de 108 olhos, que resulta em 108 classes. Para cada olho, sete imagens são capturadas em duas sessões. Três são coletadas na primeira e quatro na segunda sessão [13]. Para visualizar parte da base de dados ver Apêndice C.

Na proposta foi utilizada a totalidade de amostras da base de dados [13], incluindo mesmo aquelas amostras que não foram utilizadas em diversos trabalhos [11], [12], [84]. Elas foram desprezadas porque apresentavam resultados sem exatidão na localização e também afetavam o processo de reconhecimento. Isso mostra que o algoritmo proposto é mais bem sucedido.

Como se observa na Tab. 6.1, o algoritmo proposto conserva a exatidão do original de Masek [11], mesmo utilizando o esquema de circunferências concêntricas. Também foi feita uma comparação com o trabalho da M. Pereira [84] que usa a mesma base de dados. Ela fez melhorias na normalização e possibilitou um melhor entendimento do sistema bem como a maneira em que a localização afeta esse bloco. Os resultados mostram um aumento na exatidão geral do sistema. A comparação tanto de L. Masek [11] como da M. Pereira [84] somente foi realizada para amostras que realmente tiveram sucesso na fase de localização (ou seja, descartaram-se erros nessa fase). Na presente proposta não foi descartada nenhuma amostra. Em todos os trabalhos aqui citados utilizou-se as melhorias de deslocamentos feitas por Masek [11], [12].

Método	**FAR%**	**FRR%**	**Exatidão%**	**Tempo seg.**
L. Masek[11] (Original)	0,190	0,320	99,49%	39,35
M. Pereira [84][1]	0,036	0,220	99,74%	---
Proposto[2]	0,000	0,130	99,87%	0,074

Tab. 6.1 Comparação de sistema reconhecimento de íris, original e o proposto.

[1] Esse método baseia-se no original substituindo-se o bloco de normalização.

[2] Foi feito o experimento no mesmo computador, um após o outro.

O tempo total de processo de reconhecimento foi obtido usando-se um único

computador, resultando na coluna tempo da Tab. 6.1. Note-se que o método original utiliza a transformada de Hough com consumo de memória (matriz acumuladora) e complexidade alta para detecção de circunferências.

A Tab. 6.2 mostra uma comparação apresentada por Jiali Cui [82]. Nessa tabela, acrescentou-se o resultado do algoritmo proposto, levando-se em conta as mesmas características dos experimentos relatados nessa publicação. O algoritmo foi executado tendo-se como base aquele de Daugman implementado em Matlab por Masek [11] e modificado no módulo de segmentação. O sistema tem a configuração de um limiar igual a 0,36 tendo uma FAR=0% e um FRR=0,13%.

Método	**Exatidão**	**Tempo (segundos)**		
		Médio	**Min.**	**Max.**
Daugman	98,60%	6,56s	6,23s	6,99s
Wildes1 [95]	99,90%	8,28s	6,34s	12,54s
Wildes2 [96]	99,50%	1,98s	1,05s	2,36s
Jiali Cui	99,54%	0,2426s	0,1870s	0,3290s
Proposto[1]	**99,87**%	**0,0742**s	0,0450s	0,7950s

Tab. 6.2 Comparações de métodos para referência.

[1]Foi adicionada a linha simulando-se as mesmas características computacionais.

Na Tab. 6.2 apresenta-se o tempo médio (média arimética) de todas as comparações realizadas com as 756 imagens da base de dados. Durante os testes procurou-se os tempos mínimo e máximo. O valor máximo encontrado de 0.7950s corresponde ao primeiro teste.Após o primeiro teste, a tendência é o tempo ficar em torno do valor médio.

Pode-se ver pelas tabelas Tab. 6.1 e Tab. 6.2 que o método proposto de segmentação mostrou-se superior aos outros métodos publicados. Atingiu-se uma exatidão de 99,87% de acerto, com um tempo médio de busca de 0,0742 s. Isso representa uma melhoria de 3,27 vezes em relação ao melhor método publicado (Jiali Cui) e de 531,7 vezes em relação ao método clássico (Libor Masek).

O método de Daugman é robusto, sendo que os seus resultados são de difícil comparação, pois não são relatadas melhorias computacionais no seu método, mas os artigos mostram 100% de exatidão [37]. O esquema de reconhecimento de íris possui um bloco de localização, e ao longo do processo esse bloco permanece inalterado. Esse bloco está baseado no processo integro-diferencial e é possível se ter uma idéia do tempo de processamento desse bloco com respeito a todo um processamento de reconhecimento. Por

exemplo, Daugman em [97] apresenta uma localização que é 57,7% do total e em [52] é 20,17% do total. Daugman utiliza o mesmo processo e a mesma integro-diferencial em ambos os processos, com possíveis melhorias no último, mas esse fato não é relatado.

No algoritmo proposto, mesmo ao se inserir ruído gaussiano, ele continua sendo rápido e confiável. Isso ocorre porque as obstruções que causam problemas na localização são espalhadas, compensando a introdução de ruído. Na simulação realizada, apenas uma classe apresenta obstruções significativas (ver Fig. 6.4). Dentro dessa classe existem sete amostras, das quais quatro contêm cílios que dão erro quando não se insere um ruído gaussiano.

No décimo passo encontra-se o centro da íris. Mesmo assim, não é utilizado. Isso porque a informação da textura da íris é mais concêntrica do que a da pupila (ver Sec. 6.2.1), como se observa na amostra 52 (ver Apêndice C) da base de dados. Nesse algoritmo só foi aceita a informação útil da íris a fim de se conservar a concentricidade. A passagem para uma normalização pode estar resultando em um menor custo computacional e garantindo uma informação homogênea de uma íris. Isso porque no método proposto é feita apenas uma transformação de coordenadas polares para retangulares. Nos outros métodos, a imagem obtida em geral, apresenta muita irregularidade na concentricidade o que não ocorre no método proposto. Percebe-se que as escolhas dos limites para todas as amostras da classe 52 são semelhantes. Isso denota um bom comportamento para um processo de reconhecimento. Para um reconhecimento de uma determinada íris, a informação de entrada normalmente deverá ser a mesma. Portanto, na presente proposta se há perda de dados de textura durante a fase de localização de uma íris, esse fato ocorre também em outras sessões posteriores. Esse comportamento naturalmente é desejável. A melhoria no resultado final do sistema deve-se à melhoria na segmentação de dados, pois se toma a informação de textura mais relevante.

Para visualizar os resultados de segmentação proposta ver e o Apêndice C.

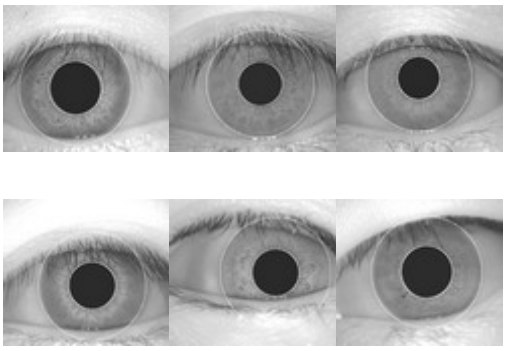


Fig. 6.8 Resposta visual do algoritmo proposto (Casia v.1).

Fig. 6.9 mostra a distribuição da distância de *Hamming* limitada em uma região onde se define o limiar. Claramente se visualiza que as duas curvas estão separadas e têm os comportamentos esperados. A escolha do limiar foi feita experimentalmente utilizando-se o módulo automatizado de teste que faz parte deste trabalho (Apêndice D.2). Utilizou-se um limiar que varia desde 0.34 até 0.47 porque tais valores geram os resultados mais coerentes. O número de comparações feitas é de 285.390. O melhor resultado corresponde ao limiar 0.39, mas o valor escolhido corresponde ao ZeroFAR com um limiar de 0.36. Isso porque comercialmente o ZeroFAR tem sido considerado a referência mais importante. No entanto, para sistemas não críticos pode-se utilizar um limiar de 0.39, pois isso resulta em uma melhoria do ponto de vista de segurança (ver).

Limiar	**Exatidão %**	**FAR %**	**FRR %**
0,34	99,795	0	0,204282
0,35	99,836	0	0,163285
0,36	**99,873**	**0**	**0,126844**
0,37	99,896	0,001752	0,101265
0,38	99,918	0,004555	0,077438
0,39	**99,925**	**0,016469**	**0,057816**
0,40	99,903	0,051859	0,044501
0,41	99,806	0,158380	0,035040
0,42	99,464	0,504923	0,027681
0,43	98,300	1,680157	0,018921
0,44	94,811	5,178177	0,010512
0,45	85,773	14,21914	0,007358
0,46	67,311	32,68510	0,003854
0,47	39,987	60,01191	0,001051

Tab. 6.4 Taxas de FAR e FRR da modificação proposta utilizando parâmetros ótimos na configuração do sistema.

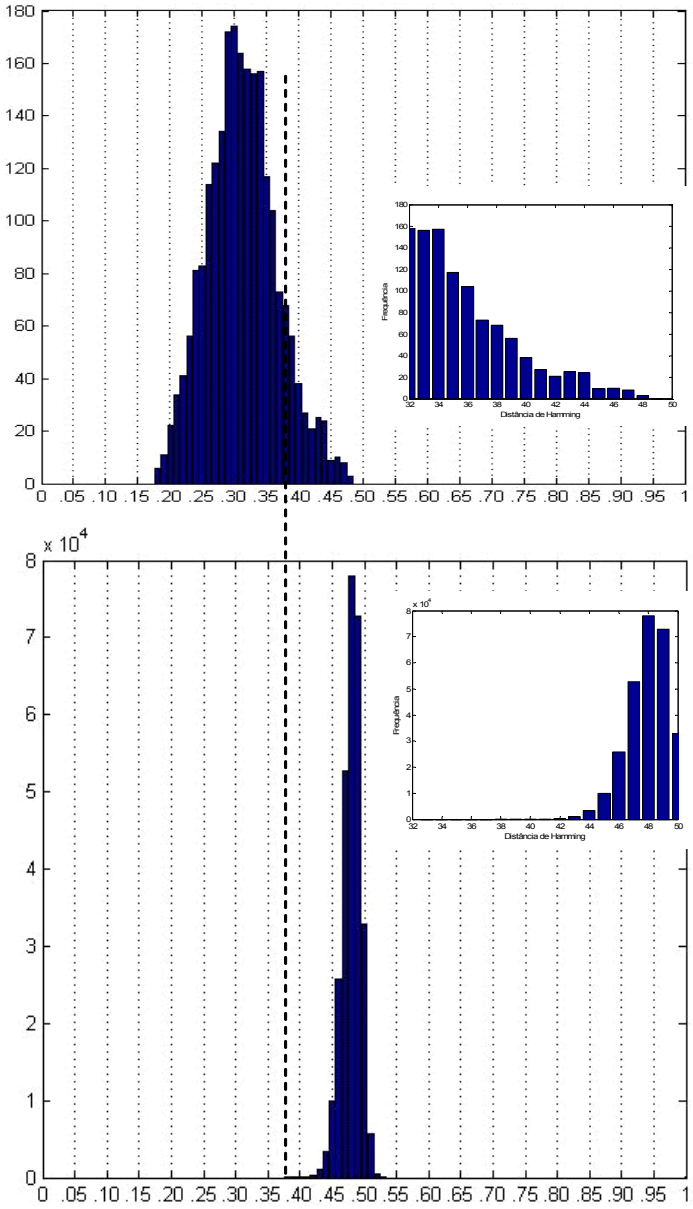


Fig. 6.9 Distribuição intra e interclasses da distância de *Hamming* usando-se a base de dados Casia v.1.

Capítulo 7

Conclusões e Trabalhos Futuros

Conclusões

A pesquisa realizada neste trabalho procura investigar os principais aspectos técnicos de um sistema biométrico de identificação pessoal, baseado em imagens de íris. Como parte do trabalho, foi programado um bloco de localização que serviu como principal ferramenta para a pesquisa. Isso confere eficiência ao sistema clássico e o torna comparável aos sistemas atuais em termos de eficiência de tempo e exatidão.

O trabalho teve também o intuito de compreender alguns métodos de reconhecimento de íris, completando a explicação disponível na literatura. As partes descritas são:

- Captura de dados: foi estudada a forma de se capturar imagens levando-se em conta parâmetros físicos que, se inseridos nas imagens, são fonte de erro em blocos subseqüentes do sistema de reconhecimento.
- *Liveness*: recomenda-se o uso desse bloco no sistema quando existe a possibilidade de que o mesmo se torne alvo de ataques. Conclui-se também que para cada tipo de ataque deve-se contar com um método de *liveness* a fim de se evitar problemas.
- Sistemas biométricos: as formas de avaliação e de aplicação a um sistema desse tipo não são triviais. Diversas características devem ser levadas em consideração, em função do interesse dos usuários finais e dos proprietários. Normalmente, o item de custo é uma das características mais relevantes.
- Sistemas biométricos baseados em íris: esses permitem customizar a implementação dos próprios sistemas de reconhecimento. Esse tipo de biometria é aplicável a grandes ou pequenas massas de usuários com alta exatidão.

O alto desempenho do bloco de segmentação construído, já é suficiente para atender muitas aplicações de segurança em tempo real, por exemplo, com o uso de um PC. Tudo indica que no futuro, poder-se-á desenvolver um produto comercial que será adicionado aos sistemas atuais já implantados. No caso do esquema proposto neste trabalho, o desempenho obtido pelo algoritmo pode ser mantido apenas no caso da base de dados Casia. Para outros tipos de captura de dados é necessária uma adaptação no algoritmo.

O indivíduo deve colocar o dispositivo de captura sobre os olhos (invasivo), o que pode causar certa rejeição por parte de usuários potenciais do sistema. Uma solução menos invasiva deve ser buscada pelos fabricantes. Até o presente momento não se têm muitos dados que suportem a construção de tais protótipos. Isso propicia novas pesquisas direcionadas a métodos não invasivos. De fato, tal invasão constitui um dos poucos problemas que a biometria de íris apresenta.

Outro ponto a ser melhorado diz respeito ao tratamento da oclusão causada por cílios e pálpebras. Esse problema é contornado pela adição de ruído gaussiano e pelo uso de filtro mediano que suaviza a imagem. Esse procedimento inicia um processo de iteração no algoritmo. A presente proposta segmenta somente informação útil (textura), rejeitando a textura do limite externo que normalmente é mais fraca (se houver). Por essa razão, mesmo aparentes deslocamentos na localização fornecem uma melhoria na exatidão do sistema.

Dessa forma, uma melhoria na localização (segmentação de textura) aumenta a eficiência do processo de reconhecimento.

Cabe mencionar por fim, que o método proposto de segmentação mostrou-se superior aos métodos publicados para localização. Atingiu-se uma exatidão de 99,87% de acerto, com um tempo médio de busca de 0,0742 s. Isso representa uma melhoria de 3,27 vezes em relação ao melhor método publicado (Jiali Cui) e de 531,7 vezes em relação ao método clássico (Libor Masek).

Se os métodos de segmentação trabalham com sucesso, pode-se obter uma informação adequada, possibilitando uma diminuição da complexidade computacional do sistema, desde que se utilize um bloco de normalização eficiente.

Os métodos de segmentação e localização são aplicados quase que na totalidade dos sistemas comerciais disponíveis, os quais são vendidos sob licença dos proprietários. A proposta de um método de segmentação inovador tornou-se um desafio motivador para realização do presente trabalho.

As biometrias bimodais no futuro serão fontes de pesquisa, pois a combinação híbrida tende a fornecer maior segurança quando se aproveitam devidamente certas vantagens individuais. Se bem combinadas, poderiam solucionar problemas atuais (*livenees*). Além disso, a fim de reduzir custos poder-se-ia usar um mesmo dispositivo de captura para diferentes biometrias.

Trabalhos futuros

O estudo aponta questões importantes a serem investigadas no prosseguimento deste trabalho. Apresenta-se a seguir possíveis extensões que podem resultar em novas linhas de pesquisa. Tem-se:

- Criar recomendações condensadas para a seleção de uma biometria ótima, baseada em características já estudadas. Aplicar essa metodologia às biometrias existentes.
- Criar um esquema de captura de dados testando-se o mesmo com dispositivos disponíveis no mercado. Avaliar o custo benefício em relação aos produtos de íris já existentes.
- Criar uma base de dados de imagens de íris utilizando-se dispositivos e parâmetros próprios procurando imitar as bases de dados já existentes.
- Criar um bloco *liveness* configurável para cada caso de possível ataque.
- Melhorar os algoritmos utilizando-se técnicas adaptativas para o ajuste de parâmetros, que neste trabalho são estáticas.
- Testar o algoritmo proposto de segmentação em outras bases de dados disponíveis.
- Parametrizar e quantificar as variáveis que identifiquem melhor a qualidade do sistema (exatidão, tempo, etc.). Um caso a ser considerado, seria o correspondente à segmentação e à localização.
- Criar algoritmos eficientes para biometrias multimodais baseados em íris, garantindo a diminuição de custo. Recomenda-se adicionar a biometria da face.

Apêndices

Apêndice A: Avaliação de Biometrias Utilizando os Critérios Descritos

A.1 Pontos por Característica

Utiliza-se uma pontuação igual a zero para a pior situação. O valor igual a dez corresponde a melhor pontuação, conforme sugerido em [35] na parte de recomendações.

A.1.1 Biometria das Impressões Digitais

As *digitais* dos dedos da mão aproximam-se da biometria ideal. Nesse caso, as maiores pontuações correspondem à maturidade e à disponibilidade. A menor pontuação refere-se ao custo em relação ao retorno do investimento ROI.

Essa biometria tem uma aceitabilidade de nove pontos, isso porque é a mais antiga dentre as biometrias ainda usadas. Não chega a ter dez pontos porque a não aceitabilidade de algumas pessoas deve-se ao fato de que tais pessoas possuem digitais similares as de outras pessoas com problemas na área criminal (*Acceptance*: 9).

As digitais são de fácil uso, sendo que com os novos sensores ergonômicos bem como com as melhorias tecnológicas, essa biometria torna-se cada vez mais simples (*Easy*: 8,5).

A diminuição dos custos dos dispositivos (destinados à coleta de digitais) aliada ao fácil uso (implantação e treinamento) torna a relação de retorno de investimento alta (ROI: 7).

A biometria é pouco invasiva e com alta maturidade, servindo-se de dispositivos pequenos e de rápida adaptação, mas com um FAR e FRR (FAR: 8, FRR: 8) que não seriam suficientes se a aplicação tem como prioridade a segurança.

A.1.2 Biometria da Face

Essa biometria está sendo muito pesquisada porque oferece ao usuário alta aceitabilidade por ser uma forma natural de medição, sendo que essa biometria é não invasiva. Possui uma baixa pontuação no ROI devido ao fato de que as câmeras melhoram com a introdução de novas tecnologias (encarecendo esse produto) e a postura para a captura varia também com a tecnologia e de acordo com o tipo de pesquisas. A Fig. A.1 mostra uma pontuação da biometria da face.

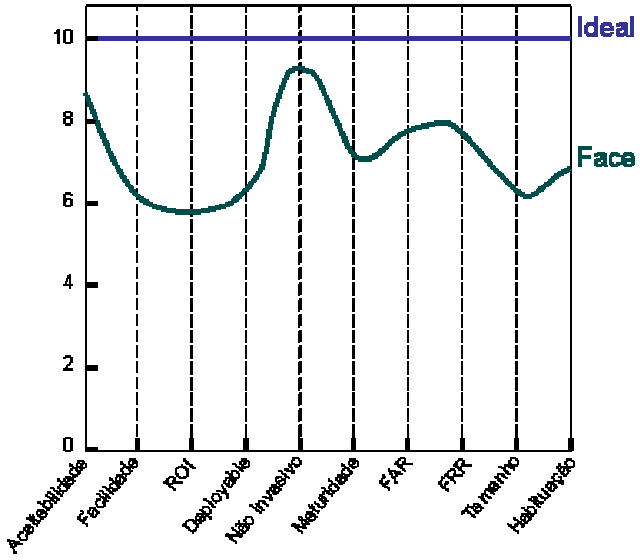


Fig. A.1 Pontuação da biometria da face [35].

Nessa biometria requer-se uma câmera digital, porém isso pode gerar problemas de transporte adequado. Isso não se deve apenas ao tamanho, mas também pela necessidade de se prover iluminação adequada. Além disso, têm-se outros fatores que variam de um ambiente a outro.

A.1.3 Biometria da Voz

Semelhante ao uso da face é também natural. Mas apresenta um problema relacionado ao fato de que o sistema responde também a um conjunto de pessoas. Além disso, a facilidade de uso está comprometida porque requer um tempo de treinamento considerável. A Fig. A.2, mostra a pontuação da biometria da voz.

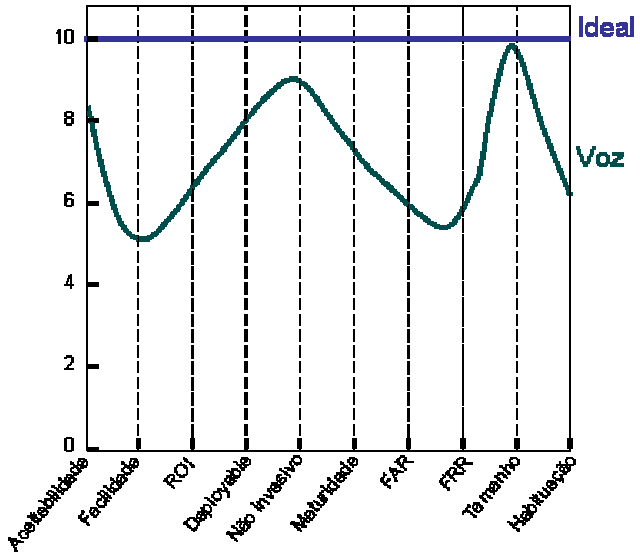


Fig. A.2 Pontuação da biometria da voz [35].

A.1.4 Biometria da Íris.

Está associada sempre a alta segurança sendo biometricamente muito atrativa. Apresenta os melhores FRR e FAR. A aceitação é baixa, devido principalmente ao fato de que é invasivo. Provoca certo desconforto de uso, devido ao medo de possíveis danos no olho. A Fig. A.3, mostra a pontuação para a biometria da íris.

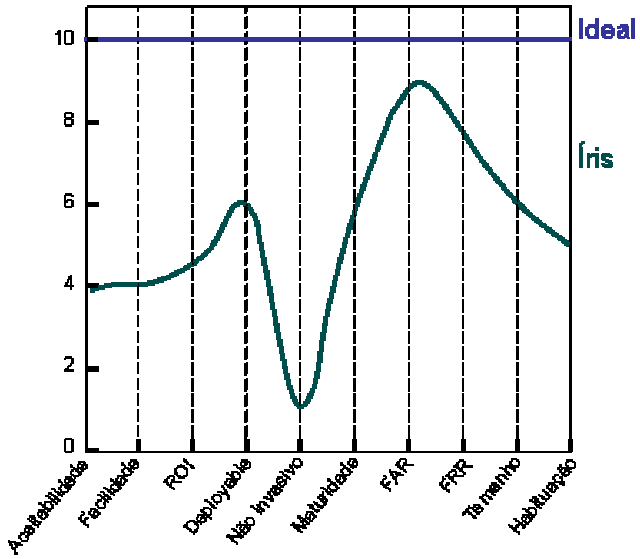


Fig. A.3 Pontuação para a biometria da íris [35].

A.2 Escolha de uma Biometria para Redes de Acesso

A biometria mais próxima da ideal para essa recomendação é a da digital de dedos. Essa escolha é baseada na pontuação de cada biometria relativa a uma ideal. Entretanto, como já foi dito, a biometria da íris mostra alta segurança, a voz e a face apresentam aceitabilidade alta e as digitais oferecem a melhor pontuação em geral.

As biometrias bimodais poderiam ser utilizadas com sucesso. No entanto, os itens referentes ao custo e à manutenção devem ser levados em conta, visando uma melhor relação entre custo e benefício.

Utilizando-se os parâmetros correspondentes aos sete pilares ou mesmo outro método descrito, pode-se perceber que existe uma possibilidade de se encontrar uma biometria ótima que atenda os requisitos da configuração exigida, estudando-se o problema e o ambiente.

Apêndice B: Descrição de Métodos

B.1 Captura de Dados

Para aumentar o nível de segurança e o desempenho, visando atrair maior interesse dos usuários e dessa forma incrementar o número de aplicações, a captura de dados é um bloco que tem sido pesquisado [76]. Facilmente, encontram-se companhias comerciais interessadas nesse tema, tais como: LG (*Life's Good*) [w23], Iridian [w24], Panasonic [w25], etc. Neste apêndice detalha-se de forma acadêmica a captura de dados. Isso foi feito devido a pouca informação disponível e ao sigilo comercial em torno dos produtos.

Para conseguir uma maior quantidade de detalhes da íris, a imagem deve ser capturada com uma alta resolução e, de preferência, utilizando-se uma luz infravermelha a fim de revelar até mesmo detalhes que não podem ser vistos apenas com a luz visível. Com comprimento de onda entre 700 - 900 nanômetros, essa faixa é considerada segura pela Academia Americana de Oftalmologia.

A imagem deve possuir uma resolução de no mínimo 70 pixels entre a borda da pupila e a borda externa da íris [61]. A distância entre o usuário e o dispositivo de aquisição depende da resolução e varia de alguns centímetros a alguns metros. O mercado tem hoje uma razoável diversidade de dispositivos que fazem a adaptação necessária para se capturar os dados de um olho (ver Fig. B.1). Porém, o custo desses dispositivos é alto, sendo uma opção mais barata a utilização de câmeras de alinhamento manual, tornando importante um posicionamento adequado do usuário [83].

Fig. B.1 Dispositivo comercial de captura de uma imagem de íris [37].

Na imagem capturada, uma **informação** normalmente não utilizada é a cor. Mesmo quando é usada por alguns autores [3], a cor não tem alto grau de importância para o reconhecimento. De fato, são mais relevantes as características angulares e concêntricas da íris, resultantes de sua estrutura [84]. Em relação à quantidade de informação, a cor confrontada com a estrutura que gera uma textura, oferece menos informação.

Muitos avanços na área comercial têm sido obtidos, mas não publicados. Artigos em que se podem encontrar uma descrição de métodos de captura foram publicados por Daugman, Li Ma, etc.

O grupo de pesquisa *Iris Capture Project* [88], realiza avanços em captura de imagens de íris para a Universidade Bath. A configuração do dispositivo é uma câmera digital de alta resolução infravermelha com ajuste de eixo e altura, com o alvo de se obter o melhor ângulo e minimizar as reflexões (ver Fig. B.2).

Fig. B.2 Equipamento ajustável para captura de imagens de íris.[88]

Os dispositivos essenciais em uma captura de imagens de íris geralmente são a câmera, a lente e o dispositivo de luz infravermelha (ver Fig B.3).

Um outro problema pesquisado de captura é o foco da imagem que requer uma distância focal padrão [76], bem como o autofoco e *zoom*

[77].

(a) (b) (c)

Fig. B.3 Componentes básicos de captura de íris. (a) Câmera digital de 1.3 Mega pixel; (b) lente; (c) Lâmpada infravermelha [88]

O dispositivo envia imagens capturadas, caso o processamento posterior não seja feito no mesmo dispositivo. Se existe uma separação física entre o dispositivo de captura e o processador então, a transmissão e o processamento de dados podem diminuir o desempenho em termos de eficiência. Há um ganho se o dispositivo de captura puder determinar se é ou não uma imagem de um olho.

As melhorias recomendadas visam obter uma base de dados mantendo-se as mesmas características de iluminação e de distância focal. Avalia-se essa base de dados como se fosse um conjunto ideal e assim obtêm-se os parâmetros ideais de limiar. Por comparação, pode-se saber que as amostras correspondem às imagens capturadas corretamente. Pode-se então, caracterizar o histograma dessas amostras [79] (ver Fig. B.4).

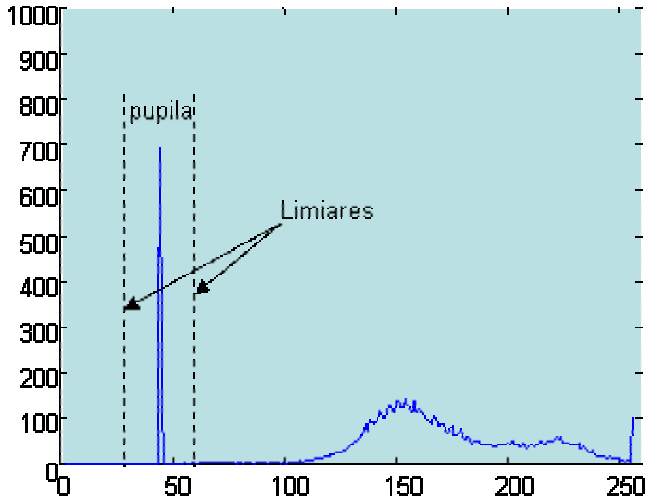


Fig. B.4 Histograma de uma amostra da base de dados Casia.

No histograma observa-se que se tem um pico na escala de cinza. Tal pico pertence a uma região do olho de tonalidade bem escura que sempre corresponde à pupila. O comportamento do histograma mais a informação de pico caracterizam um olho humano para essa base de dados. Após a obtenção das informações que são utilizadas para a criação

do BD (Banco de Dados), esses parâmetros devem ser atualizados no sistema visando o ajuste do novo BD e assim diminuir o erro de registro de novas amostras.

Os primeiros sistemas desenvolvidos usavam uma fonte de luz e câmeras de vídeo comuns. A luz comum dificulta a extração da textura da íris em olhos claros, e se fazia necessária uma equalização de histograma da imagem da íris. As abordagens mais recentes utilizam fonte de luz infravermelha e câmeras que captam esse tipo de luz (em geral, basta retirar o filtro infravermelho das câmeras convencionais). A luz infravermelha oferece boas imagens de textura, independente da cor dos olhos, e é invisível aos olhos humanos, não incomodando o usuário.

A implementação segundo Daugman utilizou (ver Fig. B.5):

- Fonte de luz infravermelha.
- Desprezo da informação de cor.
- O usuário se posiciona observando um *display* de cristal líquido.

Segundo a implementação de Wildes usou-se:

- Fonte de luz difusa e polarizada.
- Câmera sensível à baixa intensidade de luz.

O usuário se posiciona olhando para um quadrado.

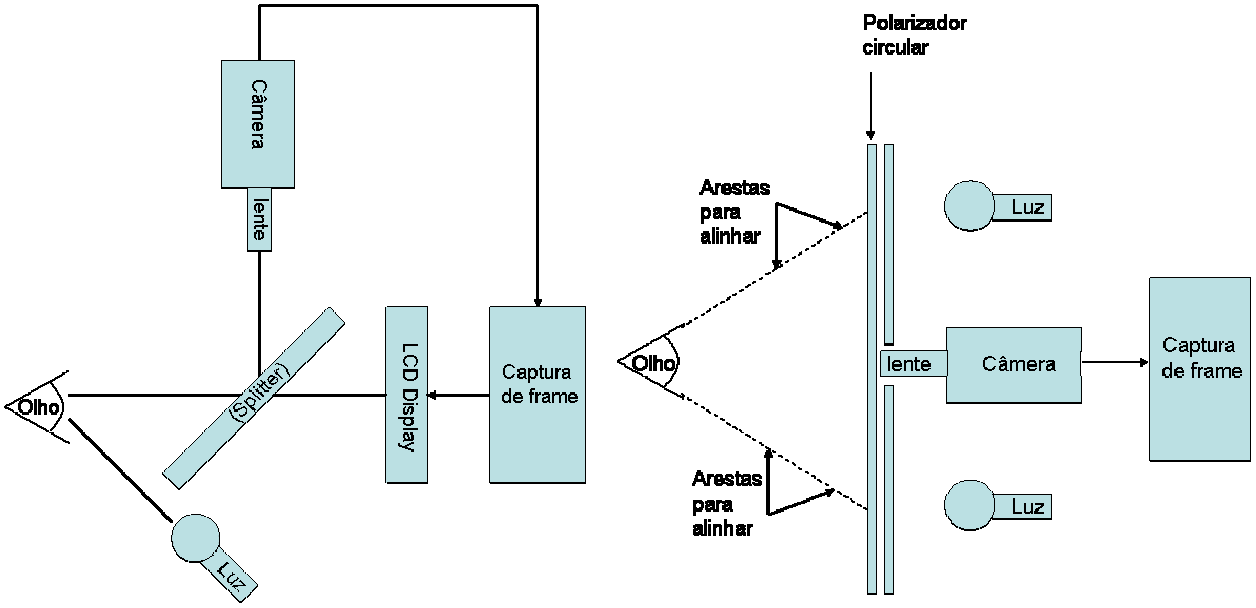


Fig. B.5 Diagrama de dispositivo de captura [6], [61].

Finalmente, têm-se outros tipos de captura de íris mais gerais, sendo que a tendência consiste em se realizar essa captura por meio de imagens que abrangem uma maior parte do

corpo, tornando assim tais sistemas menos invasivos e mais confortáveis para o usuário [80].

Outras implementações comerciais apresentam uma boa estabilidade em relação aos seus métodos de captura para reconhecimento de íris [8], apresentando taxas de erros de captura muito baixas. Hoje em dia, podem ser encontrados pelo menos seis equipamentos [8] nos quais ocorreram erros de captura, e mesmo assim as taxas de erro FAR variam entre 0,00062% e 1,76668%. A taxa de erros FRR varia entre 0,78888% e 3,548%. Todos esses resultados são muito bons e mostram uma boa robustez no tocante ao uso.

B.2 Detecção de Material Vivo - *Liveness*

Em biometria, o termo *liveness* aplica-se aos indivíduos com vida e que apresentem movimento [w26]. A vida é também o maior atributo característico de um indivíduo, porém com pouca especificidade dele mesmo, isto é, existe uma dicotomia de características entre vivo e não vivo (animado ou inanimado) [19]. Num sistema biométrico, o *liveness* somente assegura que a característica biométrica pertence a uma pessoa viva [31].

Normalmente, é desejável nos sistemas biométricos, a utilização de um detector de *liveness*. A exigência de alguma característica biométrica ao vivo visa dificultar o ataque por algum indivíduo a fim de executar uma transação ou acesso ilegal. Recentes testes acadêmicos e de mídia fazem esforços em direção ao uso dessas tecnologias biométricas a fim de tornar os sistemas baseados em biometria menos suscetíveis a ataques. De fato, nos sistemas comuns, podem ser usadas falsas impressões digitais, imagens faciais estáticas, bem como imagens de íris estáticas que substituem as amostras biométricas verdadeiras. Essas amostras fraudulentas são processadas pelo sistema biométrico e geram modelos e verificações válidas de indivíduos.

O processo de decisão de um sistema biométrico baseado em um dado *liveness* testa o seguinte algoritmo:

- Se um sistema biométrico tem "dado = ao vivo", então execute aquisição e extração. Se "dados=não ao vivo" então não faz nem aquisição nem extração.

Em outras palavras, o sistema biométrico é afinado com o detector de *livenes* ou com o oposto ou *non-liveness*. Dado que é relativamente fácil se gerar amostras falsas emulando características de vida, então, torna-se necessária também a utilização de métodos de detecção de características *non-liveness* [31].

Embora haja esforços para se desenvolver capacidades de detecção de *liveness* em todas as fases de sistemas biométricos, sempre existe a possibilidade de esses métodos serem derrotados por falsas amostras [w27].

Os métodos de detecção de *liveness* baseados em atividades fisiológicas, como sinal de

vida, levam em conta:

- Processamento de informação da biometria capturada.
- Captura de sinais de vida obtida utilizando-se hardware extra.

No primeiro caso, por exemplo, a transpiração dos dedos pode ser utilizada para se determinar a vitalidade das digitais. Um outro exemplo seria seguir o movimento da pupila.

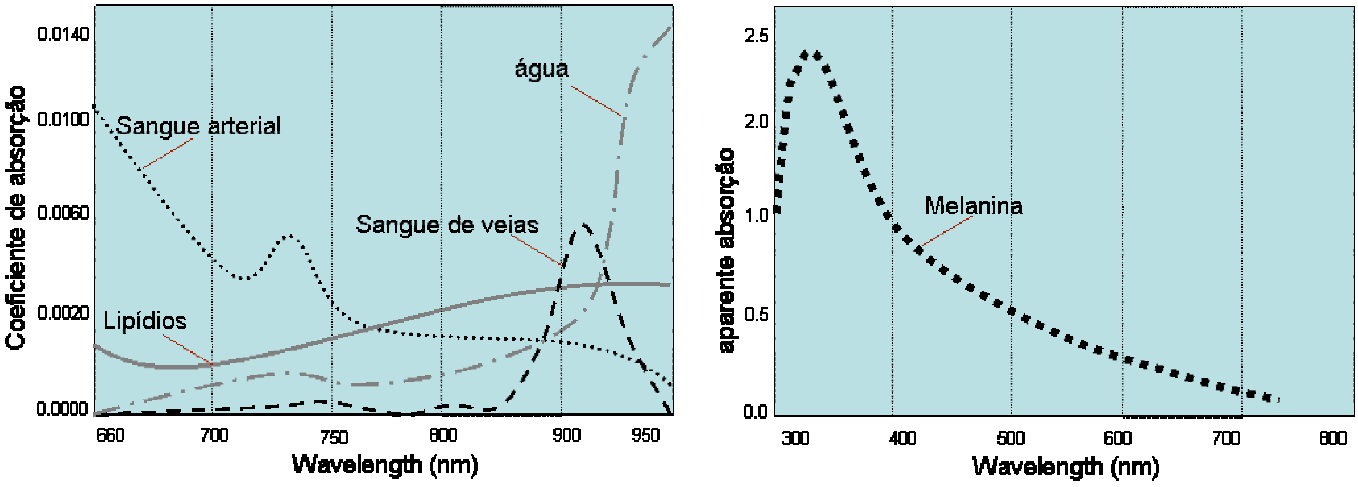
No segundo caso tem-se, por exemplo, a possibilidade de detecção de absorção de luz infravermelha por parte da íris usando-se um hardware extra para tanto (350nm) [32] .

Comercialmente, já estão disponíveis detectores de *liveness* baseados em *countermeasures*, implementados atualmente por Iridian, com certificação de *hardware* e *software* e de acordo com os 7 pilares desejáveis aos sistemas de biometria [89].

B.2.1 Métodos

Os métodos pesquisados e testados foram publicados na literatura e correspondem aos estudos de J. Daugman e de seus colaboradores [89]. Para cada possível tipo de ataque pode-se prover um possível contra ataque (*countermeasures).*

A Fig. B.6 mostra propriedades de absorção de luz das veias, artérias e melanina. As características de cada curva mostram um comportamento diferenciado no grau de absorção da melanina e de outros possíveis materiais que absorvem a luz.



(a) (a)

Fig. B.6 Propriedades de absorção de luz de materiais vivos [89].

A detecção é feita através de transformada de Fourier 2D, para se diferenciar se uma íris é natural ou uma lente de contato (ver Fig. B.7).

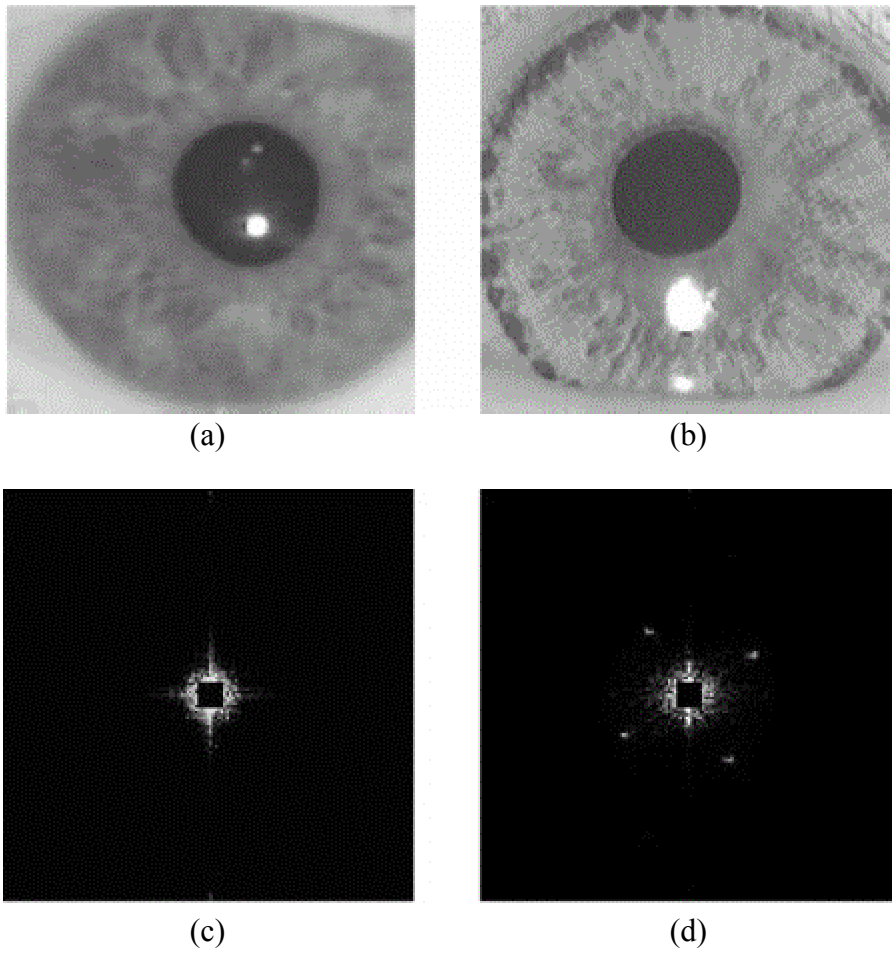


Fig. B.7 Utilização de lente de contacto e transformada de *Fourier* [89].

A luz que incide no olho é refletida na retina, fazendo com que essa cavidade óptica apareça vermelha. Isso ocorre devido à presença de veias e de sangue na retina. Tal fato pode ser aproveitado para se detectar a existência de vida (ver Fig. B.8).

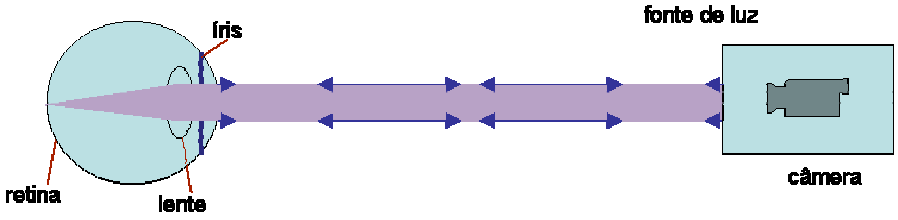


Fig. B.8 Cavidade do olho [89].

A posição de reflexão da luz na córnea e na lente do olho pode ser usada para se detectar movimento do olho. No olho natural, existem 4 superfícies ópticas que refletem a luz. Sabendo-se as posições de origem da luz, pode-se saber a posição das reflexões (ver Fig.

B.9).

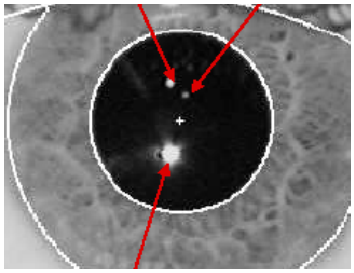
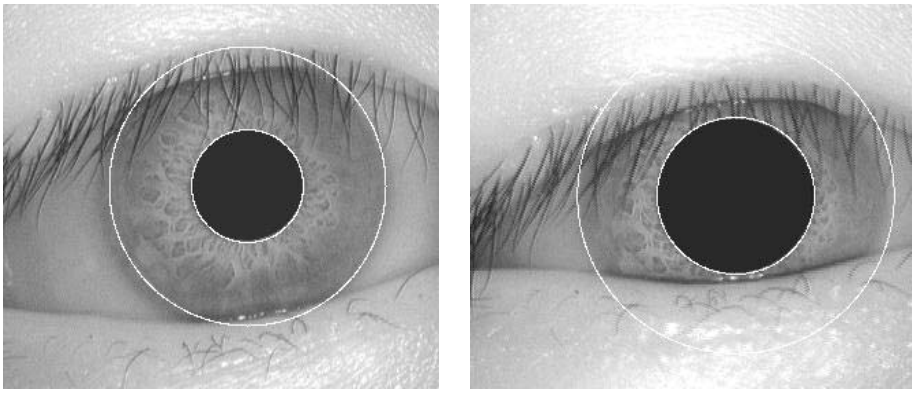


Fig. B.9 Reflexão da luz na superfície do olho é característico [89].

A Fig.B.10 mostra também uma variação do tamanho da pupila de acordo com a intensidade de luz. A Fig.B.11 mostra os valores associados ao tamanho da pupila.

Usando-se essas informações, avalia-se o comportamento involuntário, podendo-se então detectar uma movimentação da pupila provocada pelos reflexos musculares em reação à luz. A íris possui um diâmetro médio igual a 12 mm. O tamanho da pupila varia entre 10% e 80% do diâmetro da íris [52]. A Fig. B.10 mostra também uma variação do tamanho da pupila de acordo com a intensidade de luz. A Fig. B.11 mostra os valores associados ao tamanho da pupila.



(a) (b)

Fig. B.10 Pupilas. (a) Contraída; (b) Dilatada que se deforma aumentando e diminuindo a região de interesse.

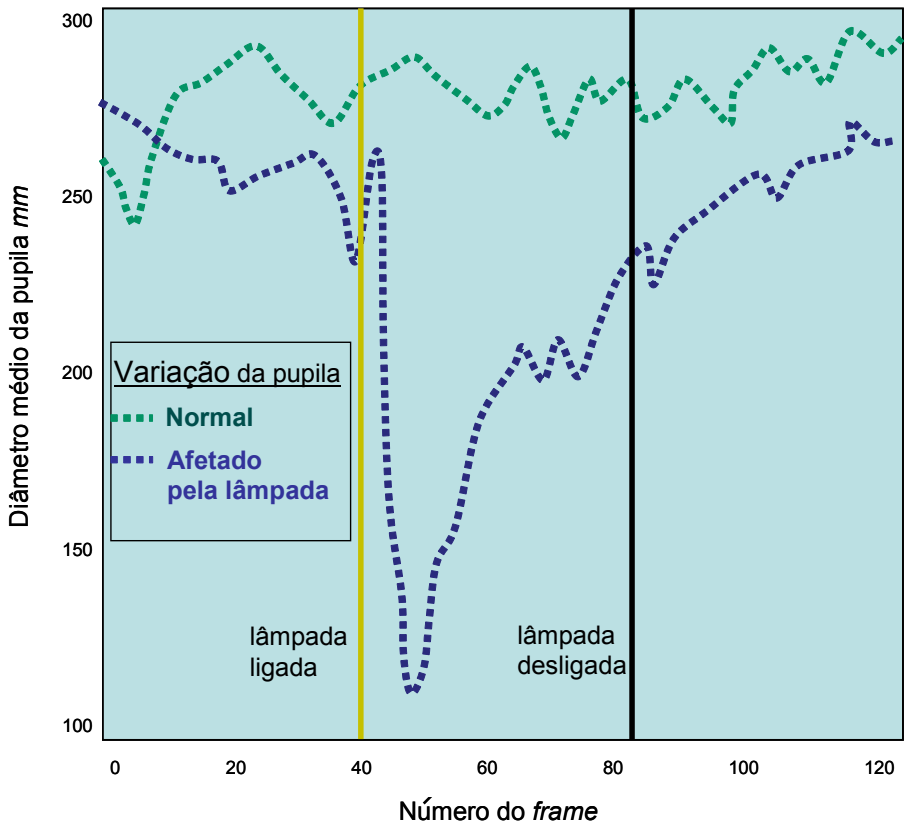


Fig. B.11 Movimento da pupila (*hippus*) utilizando uma lâmpada iluminadora [90].

Pode-se também realizar uma avaliação do comportamento voluntário que modifica, por exemplo, a posição das pálpebras de acordo com o movimento do olho.

O método utilizado também deve levar em conta o tipo de fraude que se quer evitar. Por exemplo, na Universidade de Cambridge em um experimento para se avaliar um dispositivo, utilizou-se uma foto de íris perfurada na área da pupila. O sistema aceitou como válido a íris, dado que a foto alterada passou no teste de movimentação da pupila (ver Fig. B.12). Assim é aconselhável que a detecção de material vivo ou *liveness* esteja criptografada (código ou imagem). A base de dados também deve estar protegida, sendo que o *template* ou modelo deve ser criado tendo-se em conta o dispositivo de captura, o bloco específico de obtenção de dados bem como, a aplicação específica do sistema.

Fig. B.12 Teste de anti-fraude com uma foto de íris perfurada [37].

B.3 Localização de Íris: Descrição de Métodos

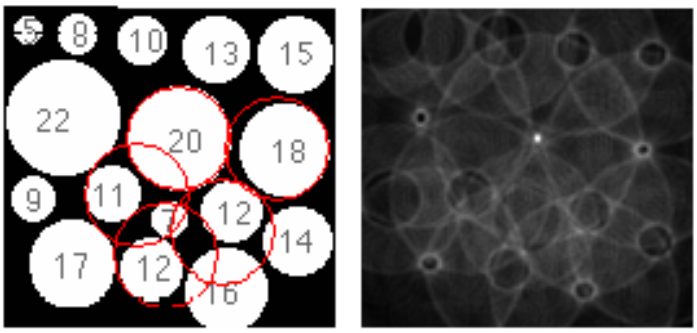
Existem muitas propostas de localização de íris, sendo que as mais utilizadas estão baseadas na detecção de circunferências. Comentam-se a seguir as técnicas de localização usadas frequentemente como: a transformada de Hough, análise de intensidades e a integro-diferencial [52].

B.3.1 Transformada de Hough

A transformada de Hough (TH) é um método padrão para detecção de *"*formas*"* que são facilmente parametrizadas, ou seja, de fórmulas conhecidas, tais como círculos em imagens digitalizadas. Essa transformada consiste em se definir um mapeamento entre o espaço de imagem (x, y) e o espaço de parâmetros (c, d, r). Tem-se:

$$(x-c)^2 + (y-d)^2 = r^2 \qquad \text{(B.1)}$$

onde *c* e *d* definem o centro do círculo e *r* é o raio. Para isso, esse espaço de parâmetros é discretizado e representado na forma de uma matriz de inteiros ou células, onde cada posição da matriz corresponde a um intervalo no espaço real de parâmetros. Procuram-se todos os círculos (c, d, r) que passam pelo ponto fixo (x, y). Mostra-se na equação B.1 um 'cone' no espaço (c, d, r) que é fixado pelos parâmetros (x, y). Deve-se então acumular todos esses cones no espaço tridimensional e buscar um pico máximo da acumulação. Se o acúmulo na célula correspondente é alto, então a célula é escolhida [91]. Na Fig. B.13, apresenta-se uma demonstração da transformada de Hough para detecção dos círculos de raio igual a 20.



(a) (b)

Fig. B.13 Detecção de círculos de raio 20, utilizando transformada de Hough [91].

A Fig.B.13(a) mostra uma imagem contendo diversas circunferências de vários tamanhos. Procura-se detectar os círculos de raio igual a 20. Na Fig.B.13(b) mostra-se uma matriz acumuladora, sendo que a maior intensidade de incidência corresponde à circunferência de raio 20.

A transformada de Hough é uma especialização da transformada de Radon. Esse domínio é um espaço tridimensional das variáveis (c, d, r), baseado em densidades e vizinhanças. A determinação da imagem tridimensional de Radon tem complexidade de $O(ND^2)$ [92], onde N é o número total de pontos e D é o quantidade de células de acumulação.

Em conjunto com uma boa detecção de bordas, a transformada de Hough é utilizada para a detecção de íris [6], [70], [71].

Cabe ressaltar que os métodos de reconhecimento de íris que usam a transformada de Hough apresentam problemas. A TH requer valores de limiar (parâmetro) que devem ser escolhidos para a detecção de bordas, e isso pode resultar na remoção de pontos críticos, causando uma falha na definição dos círculos ou arcos. Outro problema é o custo computacional muito alto devido ao fato de se usar uma aproximação através de 'força-bruta'. Por isso, a TH não é adequada para aplicações em tempo real conforme é afirmado em [107].

B.3.2 Análise de Intensidades: Operador Integro-diferencial

Para o caso específico da íris, Daugman utiliza o operador integro-diferencial dado na equação B.2 a seguir. A vantagem dessa técnica é que a mesma estima separadamente os parâmetros da íris e da pupila. Consiste em:

$$\max(r, x_0, y_0)\left| G_\sigma * \frac{\partial}{\partial r}\oint \frac{I(x,y)}{2\pi r} ds \right| \tag{B.2}$$

onde $I(x,y)$ é uma imagem contendo um olho. Nesse operador procura-se sobre o domínio (x,y) da imagem pelo valor máximo da derivada parcial em relação ao raio r, da integral normalizada do contorno da imagem ao longo de um arco circular ∂s de raio r e coordenadas do centro (x_0, y_0). A gaussiana é dada por:

$$G_\sigma = \sqrt{2\pi}^{-1} e^{-\frac{r^2}{2}} \tag{B.3}$$

e é utilizada para suavizar o ruído, com uma escala σ. O procedimento é realizado sobre três parâmetros espaciais (x_0, y_0, r) definindo-se um caminho através do contorno de integração [2], [52].

B.3.3 Algoritmos de Localização

Um dos algoritmos mais rápidos e de baixo custo computacional é a proposta de se ajuntar uma detecção de bordas e detecção de circunferências, diminuindo assim, o domínio [71]. Segundo Li Ma, primeiro faz-se uma estimativa aproximada do centro e em seguida passa-se para a forma binária, diminuindo-se a região apropriadamente. Então, aplica-se o operador de bordas e uma detecção de círculos, para se achar o centro real. Os passos do algoritmo são:

- Projetar a imagem nas direções vertical e horizontal a fim de se aproximar do centro (X_p, Y_p) da pupila. Normalmente, a pupila é de baixa intensidade e sem ruído. As coordenadas correspondem à mínima intensidade das duas projeções. Considera-se o centro da pupila como sendo o ponto (X_p, Y_p) tal que[71]:

$$X_p = \arg\min_x \left(\sum_y I(x,y) \right) \tag{B.4}$$

$$Y_p = \arg\min_y \left(\sum_x I(x,y) \right) \tag{B.5}$$

  onde $I(x,y)$ é a imagem projetada do olho.
- Compor uma imagem binária de tamanho 120x120, centrada no ponto (X_p, Y_p), e adaptando-se um limiar apropriado através do uso de um histograma dessa região. Nessa região repete-se o passo anterior e essa é a nova estimativa da pupila que deve substituir a anterior.

- Calcular os parâmetros exatos dos dois círculos aplicando-se o operador de Canny [93] para se obter as bordas e a transformada de Hough [92] [94] a fim de se detectar os círculos. Isso é feito na região determinada por (X_p, Y_p).

Camus e Wildes [95] apresentam outro método baseado em se aperfeiçoar a seguinte medida:

$$\sum_{\theta=1}^{n}\left((n-1)\left\|g_{\theta,r}\right\| - \left(\sum_{\phi=\theta+1}^{n}\left\|g_{\theta,r} - g_{\phi,r}\right\|\right) - g_{\theta,r}/8\right) \tag{B.6}$$

onde $\left\|g_{\theta,r}\right\|$ e a gradiente sobre (θ, r) da imagem normalizada. Após esse procedimento segue-se a detecção de borda usando-se uma transformada de Hough. Essa etapa não é descrita integramente pelo autor.

B.3.4 Método por Análise de Segmentação de Textura

Na referência [82] J. Cui apresenta uma aplicação de uma análise baseada na textura da íris. Apóia-se na característica de que a pupila é preta, ou seja, de baixa freqüência. Decompõe-se a imagem original usando-se a transformada de *wavelet* de Haar. A localização da pupila é facilitada usando-se a decomposição *wavelet*, e inicia-se então uma estratégia de busca fina a partir dessa informação. Depois são implementados outros passos para se encontrar a íris bem como se aplica uma modificação da transformada de Hough para se aumentar a velocidade de busca. Escolhendo-se aleatoriamente pontos do mapa de bordas, inicia-se uma busca iterativa de acordo com a equação da transformada de Hough vista anteriormente. Os resultados experimentais obtidos mostram uma redução de custo computacional.

O limite externo da íris é localizado utilizando-se o operador integro-diferencial. O operador diferencial é definido como:

$$f'(i) = f(i+1) + f(i+2) - f(i-1) - f(i-2) \tag{B.6}$$

Assim, pode-se melhorar o contraste do limite exterior da íris. Se a pupila é localizada (x_c, y_c, r), a busca do limite exterior é restrita a:

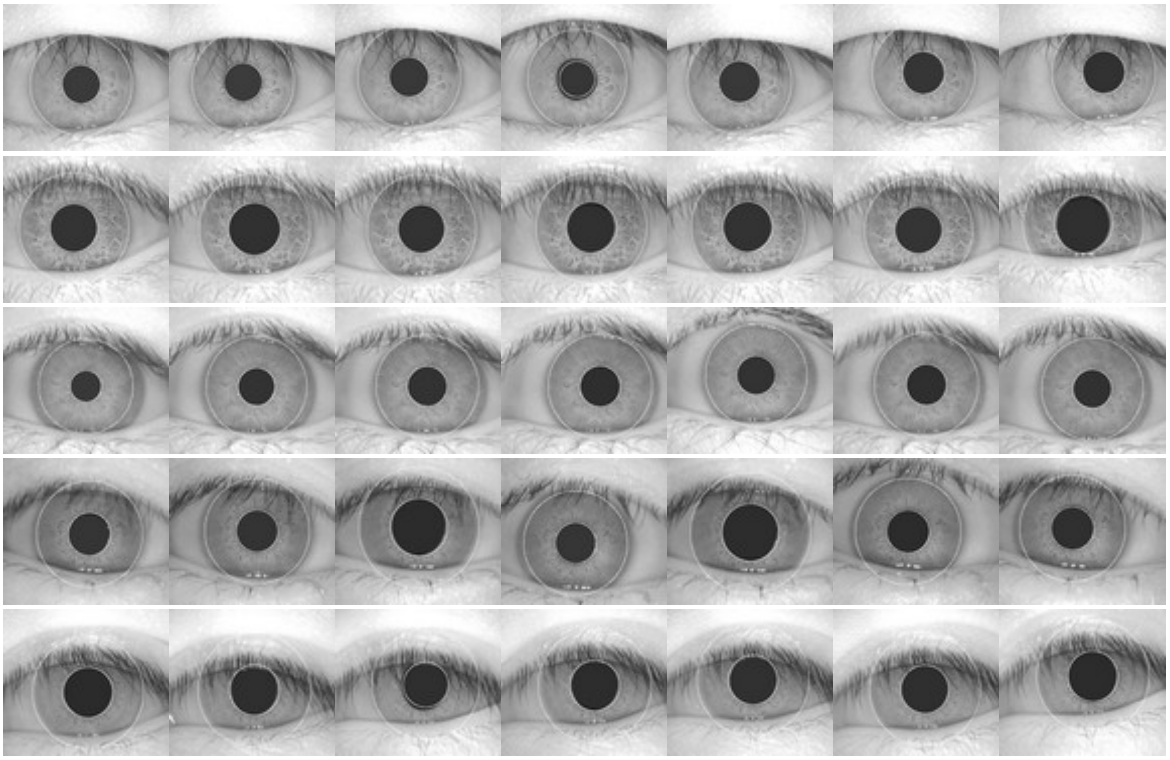
$$(x_c - x_1, y_c, r + r_1) \approx (x_c + x_1, y_c, r + r_1) \tag{B.7}$$

O método tem muita rapidez e robustez. Isso ocorre porque se utiliza um esquema simples de localização, baseado em informação local e dessa forma, minimiza-se os efeitos de ruído. Na detecção da pupila não é utilizada a transformada de Hough e isso causa uma redução do custo computacional. A aplicação do operador integro-diferencial resulta em uma melhoria do contraste. Adicionalmente, reduzem-se as necessidades de espaço, pois se passa de 3D para 2D e a busca é realizada em um domínio menor [82].

Apêndice C: Resultados da Segmentação de Íris utilizando a Base de Dados Casia

Todas as imagens testadas pertencem à base de dados Casia v.1. No entanto, somente serão apresentadas algumas imagens típicas. Para cada olho têm-se 7 amostras que estão apresentadas em uma linha (1-7) em ordem de sessão. Do lado direito, aparece um número que indica a enumeração do olho na base de dados (1-108). Os resultados obtidos no presente trabalho servem para se analisar visualmente as imagens e também para se fazer comparações com outros métodos. As imagens obtidas estão presentes em um CD anexo.

As particularidades que ocorrem em algumas imagens são apresentadas nas figuras a seguir que podem ser consideradas amostras 'difíceis'. Por exemplo, têm-se imagens com excessivas obstruções causadas pelos cílios (8, 82) ou pelas pálpebras (41, 58, 96). Outras apresentam pupila dilatada demais (62), segmentação da informação centrada perto da pupila (55), variação do tamanho da pupila (30, 55, 104) e olhos com detalhes acentuados onde os algoritmos de detecção de bordas confundem esses detalhes (19). Tem-se também íris com limite externo com pouca textura (44), íris fora de posição central esperada (45) e pupila obstruída pela pálpebra (49).



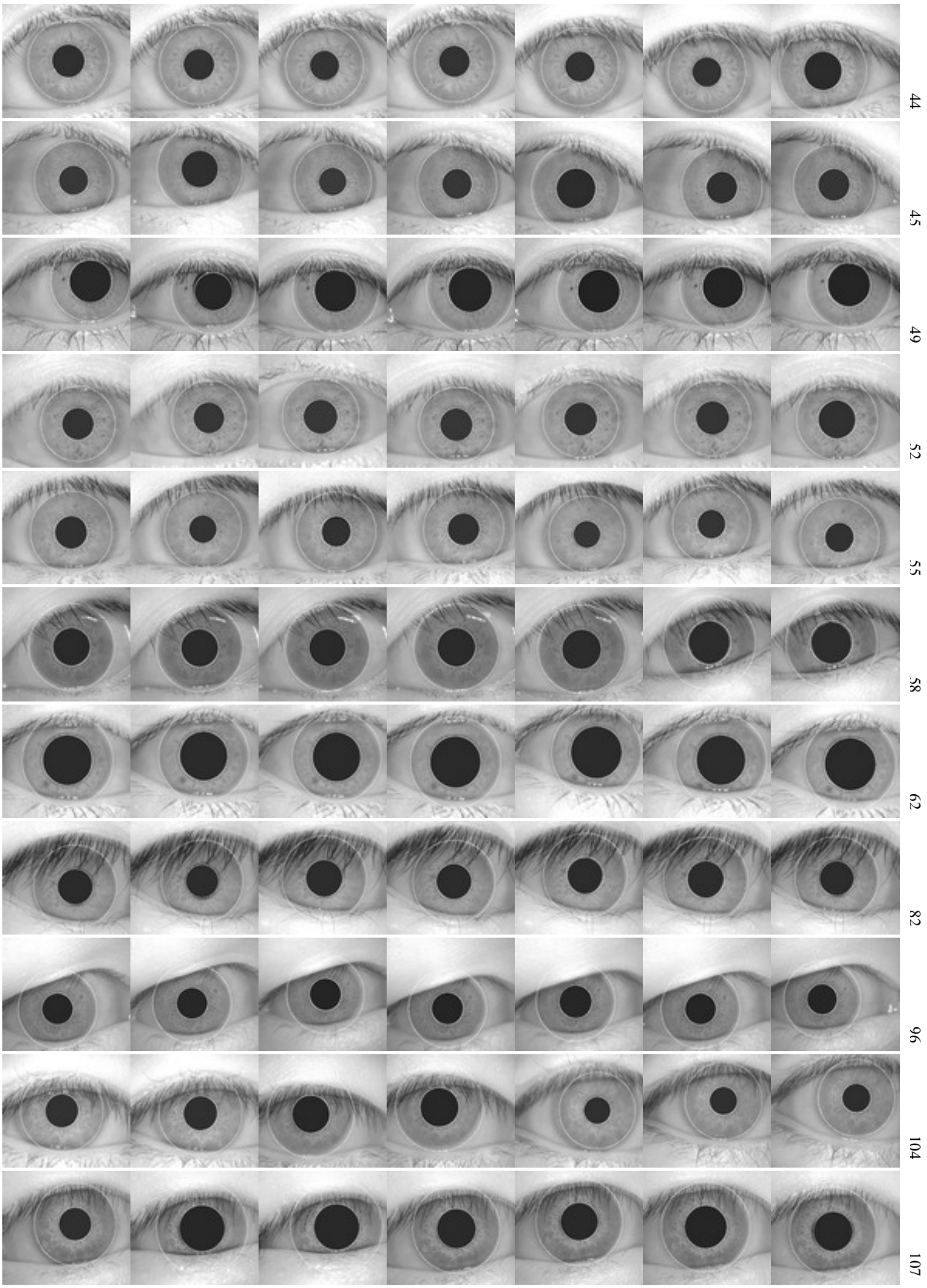


Fig. C.1 Amostras testadas da base de dados Casia.

Apêndice D: Implementação em Matlab da Localização Proposta

D.1 Implementação proposta em Matlab

A seguir apresenta-se a implementação em Matlab 6.1 de L. Masek [11]. Para a simulação do esquema proposto, substitui-se o bloco de localização. O objetivo da simulação é a obtenção de resultados que permitam uma comparação com os outros métodos existentes.

O código fonte original completo pode ser encontrado no site de L. Masek [w28], sendo que o código relativo ao bloco substituído, corresponde aos arquivos adicionados:

1. Localization.m
2. LocalizationPupil.m

Para se ativar esses arquivos na implementação é necessário tão somente se inserir no arquivo principal as linhas de programação mostradas a seguir (a palavra MODIFICAÇÃO é uma chave para se localizar onde o programa original foi modificado).

```
function [circleiris, circlepupil, imagewithnoise] =
segmentiris(eyeimage)
 . . .

%[row, col, r] = findcircle(eyeimage, lirisradius, uirisradius, scaling,
2, 0.20, 0.19, 1.00, 0.00);

[rowp1, colp1, rp1,row, col, r] =Localization(eyeimage); %MODIFICAÇÃO

circleiris = [row col r];

rowd = double(row);
cold = double(col);
rd = double(r);

irl = round(rowd-rd);
iru = round(rowd+rd);
icl = round(cold-rd);
icu = round(cold+rd);

imgsize = size(eyeimage);

. . .
```

O arquivo que executa a tarefa de segmentação da íris e da pupila é:

```
function [Xp,Yp, Rp,Xi,Yi,Ri]=Localization(image,item)

. . .

[xup,xdown,yup,ydown]=LocalizationPupil(image);

Rpx=round((xup-xdown)/2);
Rpy=round((yup-ydown)/2);

if(abs(Rpx-Rpy)>5) % parametro: erro aproximado (experimental)
    fprintf('sample: warning (add NOiSE Gaussiam)\n');
    image = imnoise(image,'gaussian',0,0.001);
    [xup,xdown,yup,ydown]=LocalizationPupil(image);
end

Xp=round((xup+xdown)/2);
Yp=round((yup+ydown)/2);

Rp=round((xup-xdown)/2); %ou 'y'
% step2 radio iris
% 40<Ri<70;


. . .

imedge=medfilt2(imedge);

for i=1:height
    j=1;
    while (imedge(i,j)==1)
        distantL=distantL+1;
        if(j<ErroRi-ErroRiin)
            j=j+1;
        else
            break;
        end
    end
    j=n2;
    while (imedge(i,j)==1)
        distantR=distantR+1;
        if(j>n2-(ErroRi-ErroRiin))
            j=j-1;
        else
            break;
        end
    end
end

Ri=(n2-(distantL+distantR)/height)/2;
Xi=Xp;(n2+(distantL-distantR)/height)/2;
Yi=Yp;
```

```
function [xup,xdown,yup,ydown]=LocalizationPupil(image)

level=0.26; %Experimental
image=medfilt2(image);
im = im2bw(image,level);

%step1 center and radio pupil
[C1,Xp]=min(sum(im'));
[C2,Yp]=min(sum(im ));

y=Yp;
yup =Yp;
while (im(Xp,yup)==0)
    yup=yup+1;
end

ydown=Yp;
while (im(Xp,ydown)==0)
    ydown=ydown-1;
end

xup=Xp;
while (im(xup,Yp)==0)
    xup=xup+1;
end

xdown=Xp;
while (im(xdown,Yp)==0)
    xdown=xdown-1;
end
```

D.2 Implementação para Automatizar o Teste

O código fonte a seguir apresentado realiza o teste automaticamente. O usuário deve indicar os parâmetros de entrada das amostras a serem testadas. Na Fig. D.1 mostra-se o diagrama de funcionamento desse módulo.

```
function rettest1=testMASEK(items,pathdatabase)
%iptsetpref('TruesizeWarning','off')
global DIAGPATH
global datatime

pathdatabase=['CASIA'];
disp('database: CASIA (only)');
    ini=items(1);
    fin=items(2);
    itemcount=1;

for item=ini:fin
    if (item<10)
        pathd1=[pathdatabase '\' '00' int2str(item) '\1'];
        path1=[pathd1 '\' '00' int2str(item)];
```

```
        pathd2=[pathdatabase '\' '00' int2str(item) '\2'];
        path2=[pathd2 '\' '00' int2str(item)];
    elseif (item<100)
        pathd1=[pathdatabase '\' '0' int2str(item) '\1'];
        path1=[pathd1 '\' '0' int2str(item)];
        pathd2=[pathdatabase '\' '0' int2str(item) '\2'];
        path2=[pathd2 '\' '0' int2str(item)];
    else
        pathd1=[pathdatabase '\' '' int2str(item) '\1'];
        path1=[pathd1 '\' '' int2str(item)];
        pathd2=[pathdatabase '\' '' int2str(item) '\2'];
        path2=[pathd2 '\' '' int2str(item)];
    end

    datatime=0;

    DIAGPATH=pathd1;
    [template, mask] = createiristemplate([ path1 '_1_1.bmp']);
        save ([ path1 '_1_1']);fprintf('\n%s>>\t',[path1
'_1_1']);fprintf('%f\t ',datatime);
    [template, mask] = createiristemplate([ path1 '_1_2.bmp']);
        save ([ path1 '_1_2']);fprintf('\n%s>>\t',[path1
'_1_2']);fprintf('%f\t ',datatime);
    [template, mask] = createiristemplate([ path1 '_1_3.bmp']);
        save ([ path1 '_1_3']);fprintf('\n%s>>\t',[path1
'_1_3']);fprintf('%f\t ',datatime);

    DIAGPATH=pathd2;
    [template, mask] = createiristemplate([ path2 '_2_1.bmp']);
        save ([ path2 '_2_1']);fprintf('\n%s>>\t',[path2
'_2_1']);fprintf('%f\t ',datatime);
    [template, mask] = createiristemplate([ path2 '_2_2.bmp']);
        save ([ path2 '_2_2']);fprintf('\n%s>>\t',[path2
'_2_2']);fprintf('%f\t ',datatime);
    [template, mask] = createiristemplate([ path2 '_2_3.bmp']);
        save ([ path2 '_2_3']);fprintf('\n%s>>\t',[path2
'_2_3']);fprintf('%f\t ',datatime);
    [template, mask] = createiristemplate([ path2 '_2_4.bmp']);
        save ([ path2 '_2_4']);fprintf('\n%s>>\t',[path2
'_2_4']);fprintf('%f\t ',datatime);
end
```

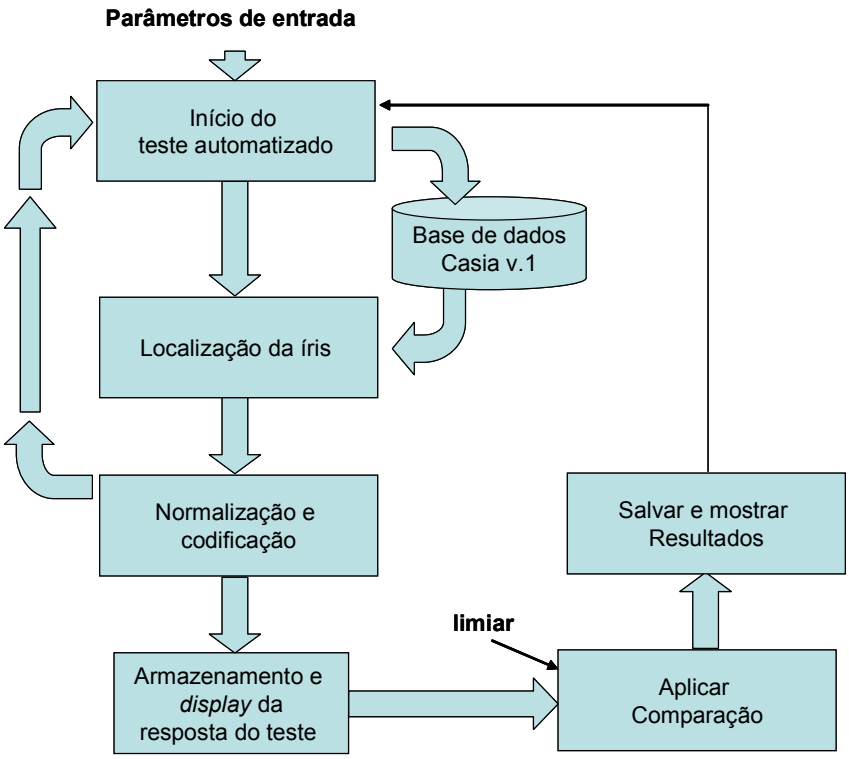


Fig. D.1 Diagrama de fluxo do módulo de teste automatizado.

D.3 Modificação do Subsistema Original

A Fig. D.2 mostra os blocos originais (Masek) que foram modificados.

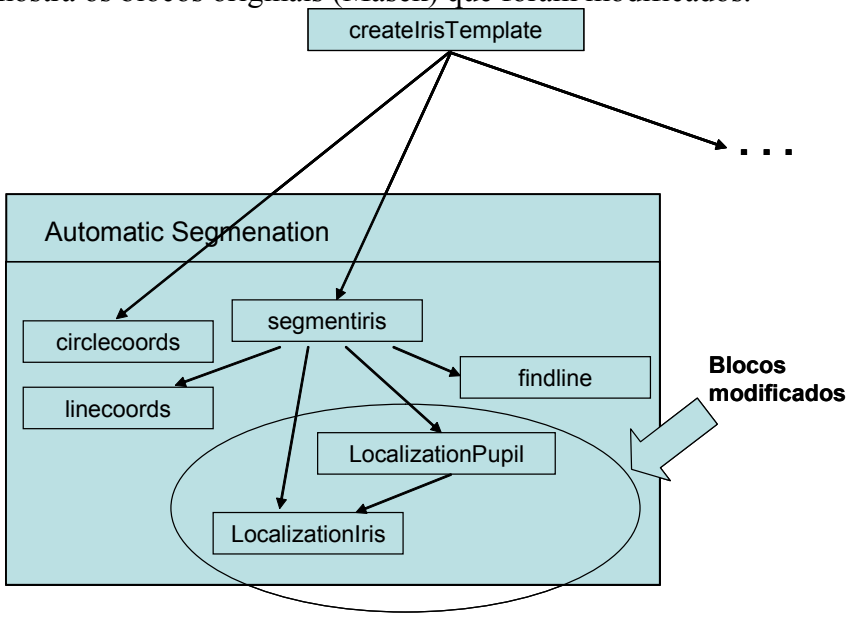


Fig. D.2 Subsistema modificado de acordo com a proposta.

Referências Bibliográficas

[1] M. Vatsa, R. Singh and P. Gupta, “Comparison of Iris Recognition Algorithms,” *IEEE Proc. of ICISIP 2004,* Índia, 2004, pp. 354-358.

[2] J. G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. Pattem Anal. Machine Intell*., vol. 15, n. 11, pp. 1148-1161, 1993.

[3] A. Bertillon, "La Couleur de l'íris," *Rev. Science*, vol. 36, n. 3, pp. 65-73. 1885.

[4] L. Flom and A. Safir, "Iris Recognition System," U.S. Patent 4641349, 1987.

[5] R. G. Johnson, "Can Iris Patterns be Used to Identify People?," Chemical and Laser Sciences Division LA-12331-PR, Los Alamos National Lab., Los Alamos, CA, 1991.

[6] R. Wildes, I. Asmuth, G. Green, S. Hsu, R Kolczynski, I Matey and S. McBride, "A Machine Vision System For Iris Recognition," *Machine Vision and Applications*, vol. 9, pp. 1-8, 1996.

[7] W. W. Boles and B. Boashash. “A Human Identification Technique Using Images of the Iris and *Wavelet* Transform,” *IEEE Trans. Signal Processing*, vol. 46, n. 4, pp. 1185-1198, April 1998.

[8] “Independent Testing of Iris Recognition Technology”, Final Report May 2005, International Biometric Group, http://www.biometricgroup.com/reports/ITIRT.html.

[9] T. Mansfield, G. Kelly, D. Chandler and J. Kane, “Biometric Product Testing Final Report,” issue 1.0, National Physical Laboratory of UK, Mar 2001.

[10] “Comparative Biometric Testing,” Round 6 Public Report Set. 2006, International Biometric Group, http://www.biometricgroup.com/reports/CBT6_report.htm.

[11] L. Masek, P. Kovesi. *MATLAB Source Code for a Biometric Identification System Based on Iris Patterns*. The School of Computer Science and *Software* Engineering, The University of Western Australia. 2003.

[12] L. Masek, “Recognition of Human Iris Patterns for Biometric Identification,” dissertação de bacharelado, Dept. The University of Western, Australia, 2003.

[13] CASIA Iris Image Database (ver 1.0), Institute of Automation, Chinese Academy of Sciences. www.sinobiometrics.com/resources.htm

[14] A. B. Ferreira, *Novo Aurélio Século XXI : O Dicionário da Língua Portuguesa*, Ed. Rio de Janeiro : Nova Fronteira, 1999.

[15] D. Ferreira, “Identificação de Pessoas por Reconhecimento de Íris Utilizando Decomposição em Sub-bandas e uma Rede Neuro-*fuzzy*,” dissertação de mestrado, Engenharia Elétrica e Computação, Dept. Comunicações, Universidade Estadual de Campinas, São Paulo, 1998.

[16] R. Hopkins, “An Introduction to Biometrics and Large Scale Civilian Identification,” *Computers & Technology*, vol. 13, n. 3, pp. 5-12. Dec. 1999.

[17] J. Wayman, A. Jain, D. Maltoni and Dario Maio, “Biometric Systems: Technology, Design and Performance Evaluation ,” Springer, Verlag, 2005.

[18] C. Costa, “Autenticação Biométrica via Teclado Numérico Baseada na Dinâmica da Digitação : Experimentos e Resultados,” dissertação de mestrado, Engenharia Elétrica e Computação, Dept. Comunicações, Universidade Estadual de Campinas, São Paulo, 2006.

[19] S. Schuckers, L. Hornak, T. Norman, R. Derakhshani and S. Parthasaradhi, “Issues for Liveness Detection in Biometrics,” *Abstract in the Proc. of the Biometrics Consortium Conference*, Arlington, VA, Sep. 2002.

[20] V. Matyas e. Z Rıha. “Biometric Authentication Systems," Tech. Report, ecom-monitor.com, 2000. www.ecom-monitor.com/papers/biometricsTR2000.pdf.

[21] A. Ross, A. Jain and S.Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Trans. on Circuit ans Systems for Vídeo Technology*, vol. 14, n. 1, pp. 4-20, Jan. 2004.

[22] K. Delac and M. Grgic, “A Survey of Biometric Recognition Methods,” *46th International Symposium Electronics in Marine*, Croatia, Jun. 2004.

[23] D. Wang, N. Chaudhadri and J. Patra. “A Constructive Unsupervised Learning Algorithm of Clustering Binary Patterns”. *IEEE International Joint Conference on Neural Networks Proceedings.* vol. 2. pp.1381-1385. 2004.

[24] S. Stern. “Integrating Biometrics into the Database and Application Server Infrastructure,” Product manager - Oracle Corporation, 2004.

[25] H. El-Bakry, “Fast Iris Detection for Personal Identification using Modular Neuronal Network,” *IEEE International Symposium on Circuits and Systems, 2001. ISCAS 2001,* Austrália, 2001, vol. 3, pp 581-585.

[26] L. Liam, A. Chekima, L. Fan and D. Dargham, “Iris Recognition Using Self-Organization Neuronal Network,” *IEEE Estudent Conference on Research and Development Proceedings*, Malaysia 2002.

[27] S. Hayken, *Redes Neurais Artificiais: Princípios e Prática*, Ed. Bookman, 2001.

[28] R. Duda and P. Hart, *Pattern Classification and Scene Analysis*, Wiley-Interscience, 1973.

[29] A. Poursaberi and B. Araabi, “A Novel Iris Recognition System Using Morphological Edge Detector and *Wavelet* Phase Features,” *ICGST International Journal on Graphics, Vision and Image Processing*, vol. 5, n. 6, Jun. 2005, pp. 9-15.

[30] C. Daouk, L. A. El-Esber, F. D. Kammoun and M. A. Alaoui, “Iris Recognition,” *Proc. of the 2nd IEEE International Symposium on Signal Processing and Information Technology, IEEE ISSPIT 2002,* Morocco, pp. 558-562, Dec. 18-21, 2002.

[31] International Biometric Group, “Liveness Detection in Biometric Systems,” Reports and Research. http://www.biometricgroup.com/reports/public/reports.

[32] J. G. Daugman, “Recognizing Persons by their Iris Patterns,” *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

[33] M. Bromba, “Bioidentification,” http://www.bromba.com/faq/biofaqe.htm#Merkmale , München, 2007.

[34] A. Jain, R. Bolle and S. Pankanti, "Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society," Kluwer, 1999.

[35] P. Reid, “Biometrics for Network Security,” Prentice Hall, Dec. 2003.

[36] Oki Electric Industry Corporation, “Oki Introduces the IRISPASS®-WG Iris Recognition System with Automatic Iris Scanning Function,” *Press Releases*, http://www.oki.com/en/press, 2002.

[37] J. G. Daugman, “Iris Recognition for Personal Identification,” *The Computer Laboratory, University of Cambridge.* http://www.cl.cam.ac.uk/~jgd1000/

[38] R. Nascimento, “Sistema de Identificação Baseada na Estrutura da Íris,” dissertação de mestrado, Dept. Engenharia Elétrica, Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2005.

[39] “Common Criteria,” Biometric Evaluation Methodology Working Group (BEMWG) 2002. http://www.cesg.gov.uk/site/ast/biometrics/media/

[40] P.J. Phillips, H. Moon, S.A. Rizvi and P.J. Rauss, “The FERET Evaluation Methodology for Face Recognition Algorithms,” *IEEE Trans. on Pattern Analysis and Machine Intelligence,* vol. 22, pp. 1090-1104, Oct. 2000.

[41] A. Jain, L. Hong and R. Bolle, “On-Line Fingerprint Verification,” *IEEE Transactions Pattern Analysis and Machine Intelligence*, vol. 19, n. 4, pp. 302-314, Abr. 1997.

[42] L. Hong, “Automatic Personal Identification Using Fingerprints”, Tech. Report, Michigan State University, Jun. 1998.

[43] E. Yu and S. Cho, “Keystroke Dynamics Identity Verification - its Problems and Practical Solutions,” *Compute & Security*, vol 23, n. 5 ,pp. 428-440, Jan. 2004.

[44] S. Slivinsky, S. Bleha and B. Hussain, “Computer-access Security Systems Using Keystroke Dynamics,” *IEEE Transactions on Pattern and Machine Intelligence*, vol. 1, n. 12, pp. 1217-1222, Dec. 1990.

[45] M. Bromba, “Biometric Myths,” Munich Technology Center, http://www.bromba.com/knowhow/biomyths.htm#DNA, 2004.

[46] “DNA Resource Report,” Applied Biosystem. http://www.dnaresource.info 2006.

[47] International Biometric Group, http://www.biometricgroup.com/.

[48] W. Shen and T. Tan, “Automated Biometrics-based Personal Identification,” *Proc. Natl. Acad. Sci*. USA. vol. 96, pp. 11065–11066, Set. 1999.

[49] Jones Road, “How It Works”, Retica Systems Inc., 2005. http://www.retica.com

[50] U.S. Government Accountability Office, “Information Security. Challenges in using Biometrics,” Sep. 2003. http://www.gao.gov

[51] P. C. Kronfeld, “The Gross Anatomy and Embryology of the Eye,” *The Eye*, H. Davson, Ed. London: Academic, vol. 1, pp. 1-66, 1968.

[52] J. G. Daugman, “How Iris Recognition Works,” *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, n. 1, pp. 21-30, 2004

[53] F. Monrose and A. D. Rubin, “Keystroke Dynamics as a Biometric for Authentication,” *Future Generation Computer Systems*, Mar. 1999.

[54] R. Joyce and G. Gupta, “Identity Authentication Based on Keystroke Latencies,” *Communications of the ACM*, Mar. 1990.

[55] L. Hong, A. K. Jain and S. Pankanti, "Can Multibiometrics Improve Performance*?," in Proc. AutoID'99*, p. 59-64. Oct. 1999.

[56] L. Kuncheva, C. Whitaker, C. Shipp and R. Duin, "Is Independence Good for Combining Classifiers?," *in Proc. Int. Conf. Pattern Recognition (ICPR)*, vol. 2, pp. 168-171, Spain, 2001.

[57] A. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. on Circuits and Systems for Video Technology,* vol. 14, n. 1, pp. 4-19, Jan. 2004.

[58] A. Jain, A. Ross, "Multibiometric Systems," *Appeared in Communication of the ACM*, Special Issue on Multimodal Interfaces, vol. 47, n. 1, pp. 34-40, Jan. 2004.

[59] K. Rhodes, “National Preparedness: Technologies to Secure Federal Buildings,” *U.S. Government Accountability Office*, Abril 2002.

[60] G. Williams, “lris Recognition Technology,” *IEEE Aerospace And Electronics Systems Magazine*, vol 12, n. 4, Abril 1997.

[61] J. G. Daugman,“High Confidence Recognition Persons by Iris Patterns,” University of Cambridge, The Computer Laboratory, 2001.

[62] J. Movellan, “Tutorial on Gabor Filters,” Machine Perception Laboratory, 2002. http://mplab.ucsd.edu/tutorials/pdfs/gabor.pdf[63] J. G. Daugman, “Uncertainty Relation for Resolution in Space, Spatial Frequency, and Orientation Optimized by Two

Dimensional Visual Cortical Filters," *Journal of the Optical Society of America*, vol. 2, n. 7, pp. 1160-1169, Jul. 1985.

[64] J. G. Daugman, "Tests of the Daugman Iris Recognition Algorithms," *The Computer Laboratory, University of Cambridge.* http://www.cl.cam.ac.uk/~jgd1000/iristests.pdf

[65] I. Daubechies, "Image Coding Using *Wavelet* Transform," *IEEE Transactions on Image Processing*, vol. 1, n. 2 ,pp. 205-220, Apr. 1992.

[66] I. Daubechies, "Where do *Wavelets* Come From? A Personal Point of View," *IEEE Journal or Magazine*, vol. 84 , n. 4, pp. 510-513, Apr. 1996.

[67] J. G. Daugman,"*Wavelet* Demodulation Codes, Statistical Independence, and Pattern Recognition," Institute of Mathematics and its Applications, Proc. 2nd IMA-IP. London: pp 244-260, 1999.

[68] W. Boles and B. Boashash "Human Identification Technique Using Images of the Iris and *Wavelet* Transform," *IEEE Transactions on Signal Processing*, vol. 46, n. 4, pp. 1185-1189, Apr. 1998.

[69] Q Minh and W. Boles, "Recognition of 2D Object Contours Using *Wavelet* Transform Zero-Crossing Representation," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 19. n. 8, Aug. 1997.

[70] L. Ma, Y. Wang and T. Tan, "Iris Recognition Using Circular Symmetric Filters," Intl. *Conf. Pattern Recognition*, vol. 2, pp. 414–417, Ago. 2002.

[71] L. Ma and T. Tan, "Personal Identification Based on Iris Texture Analysis," *IEEE Transaction on Pattern Análisis and Machine Intelligence*, vol. 25, n. 12, Dec. 2003.

[72] C. Sanchez; R. Sanchez-Reilo; "Multiscale Analysys for Iris Biometrics," *36th Annual 2002 International Carnahan Conference on Security Technology*, Las Palmas, pp. 35-38, Oct 2002.

[73] C. Sanchez and R Sanchez-Reilo, "Iris-Based Biometric Recognition Using Dyadic *Wavelet* Transform," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 17, pp.3-6, Oct. 2002.

[74] C. Tisse, "Person Identification Technique Using Human Iris Recognition," *Journal of System Research*, vol.4, pp. 67–75, 2003.

[75] S. Noh, "Multiresolution Independent Component Analysis for Iris Identification," *International Conference on Circuits/Systems Computers and Communications*, 2002.

[76] K. Park, "A Real-Time Focusing Algorithm for Iris Recognition Câmera," *IEEE Trans. On System, Man, and Cybernetics*, Part C, vol 35, n. 3, 2005.

[77] L. Xurong and X.Mei, "A Novel Algorithm Of Human Iris Recognition," *IEEE*

Proceedings of ISCIT, 2005.

[78] A. Lefohm R. Caruso, E. Reinhard, B. Budge, "An Ocularist's Approach to Human Iris Synthesys," *IEEE Computer Graphics and Applications,* vol. 26, n. 11, pp. 70-75, Dec. 2003.

[79] W. Robert, A. Ives, J. Guidry and M. Delores, "Iris Recognition Using Histogram Analysis," *IEEE Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol 1. Sec. MP8a2, pp. 562-566, Nov. 2004.

[80] G. Guo, M. Jones, P. Beardsley, "A System for Automatic Iris Capturing", Mitsubishi Electric Research Laboratories, TR2005-044. Dec. 2005.

[81] M. Erickson (1996). Eye Anatomy. *St. Luke's Cataract & Laser Institute*. http://www.stlukeseye.com/Anatomy.asp

[82] J. Cui, Y. Teniu, L. Ma, Z. Sun, "A Fast and Robust Iris Localization Method Based on Texture Segmentation," *Center for Biometric Authentication and Testing, National Laboratory of Pattern Recognition*,Chinese Academy of Sciences, Beijing, P.R.China, 2004.

[83] M Geruso, "An Analysis of the Use Iris Recognition System in U.S. Travel Document Applications," *Washington Internships for Studens of Engenieering*, Jul. 2002.

[84] M. Pereira, "Uma Proposta para o Aumento da Confiabilidade de um Sistema de Reconhecimento de Íris e sua Implementação através de Algoritmos Genéticos," dissertação de mestrado, Dept. Engenharia Elétrica, Universidade Federal de Uberlândia. 2005.

[85] R. Larico, Y. Iano e V. Sablón, "Sistema Eficiente de Reconhecimento da Íris Humana," *1º Encontro de Ciência e Tecnologia* ,Cori-Unicamp, Nov. 2005.

[86] R. F. Larico, Y. Iano e V. I. Sablón, "Processo de Reconhecimento de Íris Humana," *Rev. Ciência e Tecnologia*, UNISAL, vol. 1, n 15, ISSN 16779649. 2007.

[87] R. F. Larico, Y. Iano e V. I. Sablón, "Processo de Reconhecimento de Íris Humana: Localização Rápida de Íris," *Telecomunicações, Revista do Instituto Nacional de Telecomunicacões Inatel*, vol. 9, n. 1, Nov. 2006.

[88] Signal and Image Processing Group (2005). Iris Capture Project, Dept. Electronic and Electrical Engineering, University of Bath. http://www.bath.ac.uk/elec-eng/research/sipg/irisweb

[89] J. G. Daugman, "Iris Recognition and Anti-Spoofing Countermeasures," *7th International Biometrics Conference*, London 2004. http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf

[90] B. Toth, C. Seelen, "Liveness Detection for Iris Recognition," *NIST Workshop*,

Biometrics and E-Authentication over Open Networks. Mar. 2005.

[91] M. Schulze (2003, July 23). *Circular Hough Transform: A Java applet demonstration.* http://markschulze.net/java/hough

[92] K. Voss, H. Suesse and W. Ortmann, "Radon, Hough, Acumulación y el Método SDR," *CC/CIMAT Dep. Mathematic*, Comunicación Técnica I-04-05, 2004.

[93] J. Canny, "A Computational Approach to Edge Detection," *IEEE Trans. Pattern Anal. Machine Intell*., vol. PAMI-8, pp. 679–698, Nov. 1986.

[94] D. Ballard, "Generalized Hough Transform to Detect Arbitrary Patterns," *IEEE Trans. Pattern Anal. Machine Intell*. vol. PAMI-13, pp. 111–122, 1981.

[95] A.Camus, R. Wildes, "Reliable and Fast Eye Finding in Close-up Images," *Proceedings of the IEEE International Conference on Pattern Recognition*, 2002.

[96] R.Wildes, "Iris Recognition: An Emerging Biometric Technology," *Proceedings of the IEEE*, vol.85, pp. 1348-1363, 1997.

[97] J. G. Daugman and C. Downing, "Recognizing Iris Texture by Phase Demodulation," *IEEE Colloquium on. Image Processing for Biometric Measurement*, vol. 2, pp. 1-8. 1994.

[98] D. Anoraganingrum, "Cell Segmentation With Median Filter and Mathematical Morphology Operation," *IEEE Proceedings. International Conference on Image Analysis and Processing*, pp. 1043-1046, Itália, 1999.

[99] V. Sablón, " Processamento e Compressão do Sinal de Vídeo Utilizando a Transformada de *Wavelet*," tese de doutorado. Engenharia Elétrica e Computação, Dept. Comunicações, Universidade Estadual de Campinas, São Paulo, 2002.

[100] I. Daubechies, "Image Coding Using *Wavelet* Transform," *IEEE Transactions on Image Processing,* Apr. 1992, vol. 1, n. 2, pp.205-220.

[104] R. C. Gonzáles and R. E. Woods, "Digital Image Processing," Addison Wesley, USA 3 ed. 1992.

[105] S. Mallat, "A Theory for Multiresolution Signal Decomposition: The*Wavelet* Representation," *IEEE Transaction on Pattern analysis and Machine Intelligence*, vol. 1, n.11, pp. 674–693, Jul. 1989.

[106] S. Mallat. *A Wavelet Tour of Signal Processing*. Academic Press, Sep. 1999.

[107] C. Prado Júnior, "Biometria com Enfoque em Reconhecimento de Íris," trabalho de Bacharelado, Dept. Ciência da Computação Universidade Estadual de Londrina, Nov. 2005.

[108] K. R. Castleman, "Digital Image Processing," Ed. New Jersey: Prentice-Hall, 1996.

Sites de Consulta

[w1] Notícias Tecnologia, http://www.link.estadao.com.br/index.cfm?id_conteudo = 345 (01/2005)

[w2] Sicaman Inc., "Nuevas Tecnologias: Biocontrol," http://www.sicaman-nt.com/productos /biocontrol2.asp?id=1 (01/2007)

[w3] ISC Seguridad Informática, http://www.isc-consultores.com (01/2007)

[w4] INC Biometric Technology. "How Accurate is the Biometric?," http://bio-tech-inc.com/How_Accurate_Is_The_Biometric.htm (01/2007)

[w5] BioDisk 2.0 Biometric USB Flash Drive Fingerprint & Password Access control. http://www.card-media.co.uk/resellers/biodisk+usb2.htm (01/2007)

[w6] Bundesamt fur Sicherheit der Informationstechnik Study, "Evaluation of Fingerprint Recognition Technologies BioFinger," http://www.bsi.de/english/publications/studies/BioFinger.pdf (08/2004)

[w7] I/O Software, http://www.iosoftware.com/ (01/2007)

[w8] Idex, http://www.idex.no/ (01/2007)

[w9] I/O Software, http://www.iosoftware.com/ (01/2007)

[w10] Idex, http://www.idex.no/ (01/2007)

[w11] Recognition Systems, http://www.recogsys.com/ (01/2007)

[w12] Recognition Systems, http://www.recogsys.com/ (01/2007)

[w13] EyeDentify, http://www.eyedentify.com/ (1/2007)

[w14] LG Electronics / Íris Technology Division, http://www.lgiris.com/iris/compares.html (01/2007)

[w15] Iridian Technologies, "Selected Case Studies," http://www.iridiantech.com/solutions.php?page=2#saudi (01/2007)

[w16] CESG The National Technical Authority, http://www.cesg.gov.uk/ (01/2007)

[w17] http://gl.wikipedia.org/wiki/Iris,_Identificaci%C3%B3n_biom%C3%A9trica (01/2007)

[w18] The Children's Identification and Location Database (CHILD),

http://www.thechildproject.org/ (01/2007)

[w19] POLITEC, Biometria, "A Ficção Científica chega até a Vida," http://www.politec.com.br/portfolio/tecnologias/biometria (01/2007)

[w20] Laboratório de Neurocomputação e Computação Emergente, INPE-UBC, http://www.lac.inpe.br/~tavares/lab_inpe_ubc.htm (01/2007)

[w21] "Process of Recognition of Human Iris: Fast Segmentation of the Iris," http://www.decom.fee.unicamp.br/~rlarico/iris/localizationiris.pdf (01/2007)

[w22] "Método Rápido de Sincronismo de Símbolo em Tempo e Ajuste de Freqüência em Sinais OFDM," http://www.decom.fee.unicamp.br/~rlarico/SincronismoOFDM.pdf (01/2007)

[w23] LG Electronics / Íris Technology Division, "How it Compares," http://www.lgiris.com/iris/compares.html (01/2007)

[w24] Iridian Technologies Inc, http://www.iridiantech.com (01/2007)

[w25] Panasonic Corporation of North América, http://www.panasonic.com/cctv/products/biometrics.asp (01/2007)

[w26] Workdreference, http://www.wordreference.com/definition/liveness (01/2007)

[w27] "Biometric Access Protection Devices and their Programs Put to the Test," http://www.heise.de/ct/english/02/11/114/ (11/2002)

[w28] L. Masek, "Iris Recognition," http://www.csse.uwa.edu.au/~pk/studentprojects/libor (11/2003)

[w26] National Geographic Magazine,"A Perfect Match," Special Report http://magma.nationalgeographic.com/ngm/afghangirl (01/2007)